VVT
ISO 27001:2013 & NEN 7510:2017
Broad Horizon BV

CLASSIFICATIE: PUBLIEKELIJK

Versie V.1.5, 08-08-2019

Voorwoord

Voor u ligt de verklaring van toepasselijkheid van Broad Horizon BV, welke betrekking heeft op de werkmaatschappijen True BV en True Workspace BV.
De gekozen maatregelen in deze verklaring van toepasselijkheid zijn als best-practises geselecteerd naar aanleiding van de risicobeoordeling en de hier uit voortvloeiende geïdentificeerde risico's. Ook kan een maatregel aanvullend geselecteerd zijn vanuit wetgevende, danwel contractuele verplichtingen. De volgende codes worden daarom in deze verklaring van toepasselijkheid gebruikt:

- W: Wetgevende verplichting
- C: Contractuele verplichting
- R & B: Geselecteere best-practise nav geïdentificeerd risico.

Dit document bevat een verwijzing naar de beheerdoelstellingen en maatregelen uit bijlage A van de ISO 27001:2013 norm & NEN 7510:2017, welke voor Broad Horizon BV zijn geimplementeerd, conform de scope van de certificering. De volgorde van de maatregelen, zoals gepresenteerd in de ISO 27001:2013 norm (bijlage A), is in dit document aangehouden. Tevens is er een mapping gemaakt naar de NEN 7510:2017 normering (bijlage A).
Voor een zo volledig mogelijke dekking van het ISMS (Information Security Management System) binnen de bedrijfsvoering van de organisatie en de geboden services aan haar klanten heeft de directie er voor gekozen om zo veel mogelijk beheersmaatregelen uit bijlage A van de ISO 27001:2013 en de NEN 7510:2017 norm in scope te plaatsen van betreffende certificering. Voor een aantal gevallen bleek het echter niet mogelijk om betreffende NEN 7510:2017 maatregel te selecteren, voor deze maatregelen is een uitleg gegeven.

Aan de Verklaring van toepasselijkheid kunnen geen rechten ontleend worden. Voor uw overeenkomst met True BV, True Workspace BV verwijzen wij u naar betreffend overeengekomen contract.

Verklaring van toepasselijkheid

Norm	Maatregel	Omschrijving maatregel	Van toepassing	Maatregel geïmplementeerd	Reden selectie	Reden uitsluiting
ISO 27001:2013	**A.5.1.1**	Beleidsregels voor informatiebeveiliging	Ja	Ja	R & B	
NEN 7510:2017	**A.5.1.1**	Beleidsregels voor informatiebeveiliging	Ja	Ja	R & B	
ISO 27001:2013	**A.5.1.2**	Beoordeling van het informatiebeveiligingsbeleid	Ja	Ja	R & B	
NEN 7510:2017	**A.5.1.2**	Beoordeling van het informatiebeveiligingsbeleid	Ja	Ja	R & B	
ISO 27001:2013	**A.6.1.1**	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja	C, R & B	
NEN 7510:2017	**A.6.1.1**	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	Ja	C, R & B	
ISO 27001:2013	**A.6.1.2**	Scheiding van taken	Ja	Ja	R & B	
NEN 7510:2017	**A.6.1.2**	Scheiding van taken	Ja	Ja	R & B	
ISO 27001:2013	**A.6.1.3**	Contact met overheidsinstanties	Ja	Ja	W, C, R & B	
NEN 7510:2017	**A.6.1.3**	Contact met overheidsinstanties	Ja	Ja	W, C, R & B	
ISO 27001:2013	**A.6.1.4**	Contact met speciale belangengroepen	Ja	Ja	R & B	
NEN 7510:2017	**A.6.1.4**	Contact met speciale belangengroepen	Ja	Ja	R & B	
ISO 27001:2013	**A.6.1.5**	Informatiebeveiliging in projectbeheer	Ja	Ja	R & B	
NEN 7510:2017	**A.6.1.5**	Informatiebeveiliging in projectbeheer	Nee	Nee		We houden bij projecten bij True, waarbij het verwerken van persoonlijke gezondheidsinformatie gepaard gaat, niet expliciet rekening met patiëntveiligheid als specifiek projectrisico
ISO 27001:2013	**A.6.2.1**	Beleid voor mobiele apparatuur	Ja	Ja	R & B	
NEN 7510:2017	**A.6.2.1**	Beleid voor mobiele apparatuur	Nee	Nee		True levert op dit moment geen mobile device management diensten aan klanten actief in de zorgsector. Het beoordelen van specifieke risico's met betrekking tot de inzet van mobile devices met toegang tot persoonlijke gezondheidsinformatie heeft daardoor momenteel geen toegevoegde waarde. De mobile devices die True aan haar personeel aanbiedt worden niet ingezet om persoonlijke gezondheidsinformatie te raadplegen.
ISO 27001:2013	**A.6.2.2**	Telewerken	Ja	Ja	R & B	

NEN 7510:2017	**A.6.2.2**	Telewerken	Ja	Ja	R & B	
ISO 27001:2013	**A.7.1.1**	Screening	Ja	Ja	R & B	
NEN 7510:2017	**A.7.1.1**	Screening	Nee	Nee		True geeft geen invulling aan de toevoeging uit de zorgspecifieke implementatierichtlijnen, deze is praktisch voor zorgverleners, maar niet wenselijk voor True.
ISO 27001:2013	**A.7.1.2**	Arbeidsvoorwaarden	Ja	Ja	C, R & B	
NEN 7510:2017	**A.7.1.2**	Arbeidsvoorwaarden	Ja	Ja	C, R & B	
ISO 27001:2013	**A.7.2.1**	Directieverantwoordelijkheden	Ja	Ja	R & B	
NEN 7510:2017	**A.7.2.1**	Directieverantwoordelijkheden	Ja	Ja	R & B	
ISO 27001:2013	**A.7.2.2**	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja	Ja	R & B	
NEN 7510:2017	**A.7.2.2**	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja	Ja	R & B	
ISO 27001:2013	**A.7.2.3**	Disciplinaire procedure	Ja	Ja	C, R & B	
NEN 7510:2017	**A.7.2.3**	Disciplinaire procedure	Ja	Ja	C, R & B	
ISO 27001:2013	**A.7.3.1**	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Ja	Ja	C, R & B	
NEN 7510:2017	**A.7.3.1**	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Ja	Ja	C, R & B	
ISO 27001:2013	**A.8.1.1**	Inventariseren van bedrijfsmiddelen	Ja	Ja	C, R & B	
NEN 7510:2017	**A.8.1.1**	Inventariseren van bedrijfsmiddelen	Ja	Ja	C, R & B	
ISO 27001:2013	**A.8.1.2**	Eigendom van bedrijfsmiddelen	Ja	Ja	C, R & B	
NEN 7510:2017	**A.8.1.2**	Eigendom van bedrijfsmiddelen	Ja	Ja	C, R & B	
ISO 27001:2013	**A.8.1.3**	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja	Ja	C, R & B	
NEN 7510:2017	**A.8.1.3**	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja	Ja	C, R & B	
ISO 27001:2013	**A.8.1.4**	Teruggeven van bedrijfsmiddelen	Ja	Ja	C, R & B	
NEN 7510:2017	**A.8.1.4**	Teruggeven van bedrijfsmiddelen	Nee	Nee		True medewerkers hebben geen persoonlijke gezondheidsinformatie in bezit. True doet daarom niets extra's dan in ISO 27001 bepaalde maatregel A.8.1.4. Devices worden bij vertrek personeel gewiped.

ISO 27001:2013	**A.8.2.1**	Classificatie van informatie	Ja	Ja	R & B	
NEN 7510:2017	**A.8.2.1**	Classificatie van informatie	Nee	Nee		True maakt in de praktijk geen onderscheid in type klantdata (bijv. persoonlijke gezondheidsinformatie of andersoortige informatie) en heeft daarmee geen aanvullende maatregelen genomen naast conformering aan de ISO 27001 A.8.2.1 bepaling.
ISO 27001:2013	**A.8.2.2**	Informatie labelen	Ja	Ja	R & B	
NEN 7510:2017	**A.8.2.2**	Informatie labelen	Nee	Nee		True kan deze zorgspecifieke maatregel niet namens haar klanten borgen. True faciliteert enkel de omgeving waar betreffend gezondheidsinformatiesysteem: • op draait , danwel; • via benaderbaar is.
ISO 27001:2013	**A.8.2.3**	Behandelen van bedrijfsmiddelen	Ja	Ja	R & B	
NEN 7510:2017	**A.8.2.3**	Behandelen van bedrijfsmiddelen	Ja	Ja	R & B	
ISO 27001:2013	**A.8.3.1**	Beheer van verwijderbare media	Ja	Ja	R & B	
NEN 7510:2017	**A.8.3.1**	Beheer van verwijderbare media	Ja	Ja	R & B	
ISO 27001:2013	**A.8.3.2**	Verwijderen van media	Ja	Ja	C, R & B	
NEN 7510:2017	**A.8.3.2**	Verwijderen van media	Ja	Ja	C, R & B	
ISO 27001:2013	**A.8.3.3**	Media fysiek overdragen	Ja	Ja	R & B	
NEN 7510:2017	**A.8.3.3**	Media fysiek overdragen	Ja	Ja	R & B	
ISO 27001:2013	**A.9.1.1**	Beleid voor toegangsbeveiliging	Ja	Ja	R & B	
NEN 7510:2017	**A.9.1.1**	Beleid voor toegangsbeveiliging	Ja	Ja	R & B	
ISO 27001:2013	**A.9.1.2**	Toegang tot netwerken en netwerkdiensten	Ja	Ja	R & B	
NEN 7510:2017	**A.9.1.2**	Toegang tot netwerken en netwerkdiensten	Ja	Ja	R & B	
ISO 27001:2013	**A.9.2.1**	Registratie en afmelden van gebruikers	Ja	Ja	R & B	
NEN 7510:2017	**A.9.2.1**	Registratie en afmelden van gebruikers'	Ja	Ja	R & B	
ISO 27001:2013	**A.9.2.2**	Gebruikers toegang verlenen	Ja	Ja	R & B	

NEN 7510:2017	**A.9.2.2**	Gebruikers toegang verlenen	Nee	Nee		True Workspace registreert welke gebruikers toegang krijgen tot welke applicaties, maar niet bij welke applicaties persoonlijke gezondheidsinformatie gemoeid is.
ISO 27001:2013	**A.9.2.3**	Beheren van speciale toegangsrechten	Ja	Ja	R & B	
NEN 7510:2017	**A.9.2.3**	Beheren van speciale toegangsrechten'	Ja	Ja	R & B	
ISO 27001:2013	**A.9.2.4**	Beheer van geheime authenticatie-informatie van gebruikers	Ja	Ja	R & B	
NEN 7510:2017	**A.9.2.4**	Beheer van geheime authenticatie-informatie van gebruikers	Ja	Ja	R & B	
ISO 27001:2013	**A.9.2.5**	Beoordeling van toegangsrechten van gebruikers	Ja	Ja	R & B	
NEN 7510:2017	**A.9.2.5**	Beoordeling van toegangsrechten van gebruikers	Nee	Nee		True kan vanuit haar dienstverlening niet inspelen op de zorgspecifieke beheersmaatregel welke vereist dat er rekening wordt gehouden met gebruikers welke noodzorg verlenen en vandaaruit toegang tot persoonlijke gezondheidsinformatie dienen te hebben, zonder dat de client daarmee heeft ingestemd.
ISO 27001:2013	**A.9.2.6**	Toegangsrechten intrekken of aanpassen	Ja	Ja	R & B	
NEN 7510:2017	**A.9.2.6**	Toegangsrechten intrekken of aanpassen	Ja	Ja	R & B	
ISO 27001:2013	**A.9.3.1**	Geheime authenticatie-informatie gebruiken	Ja	Ja	R & B	
NEN 7510:2017	**A.9.3.1**	Geheime authenticatie-informatie gebruiken	Ja	Ja	R & B	
ISO 27001:2013	**A.9.4.1**	Beperking toegang tot informatie	Ja	Ja	R & B	
NEN 7510:2017	**A.9.4.1**	Beperking toegang tot informatie	Nee	Nee		True speelt geen rol in het faciliteren van MFA verplichtingen om toegang tot de applicatie te krijgen op gebruikersniveau. Tevens kan True niet de verantwoordelijkheid voor de klant nemen om deze applicaties te isoleren ten opzichte van andere systemen.
ISO 27001:2013	**A.9.4.2**	Beveiligde inlogprocedures	Ja	Ja	R & B	
NEN 7510:2017	**A.9.4.2**	Beveiligde inlogprocedures	Ja	Ja	R & B	
ISO 27001:2013	**A.9.4.3**	Systeem voor wachtwoordbeheer	Ja	Ja	R & B	
NEN 7510:2017	**A.9.4.3**	Systeem voor wachtwoordbeheer	Ja	Ja	R & B	
ISO 27001:2013	**A.9.4.4**	Speciale systeemhulpmiddelen gebruiken	Ja	Ja	R & B	

NEN 7510:2017	**A.9.4.4**	Speciale systeemhulpmiddelen gebruiken	Ja	Ja	R & B
ISO 27001:2013	**A.9.4.5**	Toegangsbeveiliging op programmabroncode	Ja	Ja	R & B
NEN 7510:2017	**A.9.4.5**	Toegangsbeveiliging op programmabroncode	Ja	Ja	R & B
ISO 27001:2013	**A.10.1.1**	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja	Ja	R & B
NEN 7510:2017	**A.10.1.1**	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ja	Ja	R & B
ISO 27001:2013	**A.10.1.2**	Sleutelbeheer	Ja	Ja	R & B
NEN 7510:2017	**A.10.1.2**	Sleutelbeheer	Ja	Ja	R & B
ISO 27001:2013	**A.11.1.1**	Fysieke beveiligingszone	Ja	Ja	C, R & B
NEN 7510:2017	**A.11.1.1**	Fysieke beveiligingszone	Ja	Ja	C, R & B
ISO 27001:2013	**A.11.1.2**	Fysieke toegangsbeveiliging	Ja	Ja	R & B
NEN 7510:2017	**A.11.1.2**	Fysieke toegangsbeveiliging	Ja	Ja	R & B
ISO 27001:2013	**A.11.1.3**	Kantoren, ruimten en faciliteiten beveiligen	Ja	Ja	R & B
NEN 7510:2017	**A.11.1.3**	Kantoren, ruimten en faciliteiten beveiligen	Ja	Ja	R & B
ISO 27001:2013	**A.11.1.4**	Beschermen tegen bedreigingen van buitenaf	Ja	Ja	R & B
NEN 7510:2017	**A.11.1.4**	Beschermen tegen bedreigingen van buitenaf	Ja	Ja	R & B
ISO 27001:2013	**A.11.1.5**	Werken in beveiligde gebieden	Ja	Ja	R & B
NEN 7510:2017	**A.11.1.5**	Werken in beveiligde gebieden	Ja	Ja	R & B
ISO 27001:2013	**A.11.1.6**	Laad- en loslocatie	Ja	Ja	R & B
NEN 7510:2017	**A.11.1.6**	Laad- en loslocatie	Ja	Ja	R & B
ISO 27001:2013	**A.11.2.1**	Plaatsing en bescherming van apparatuur	Ja	Ja	R & B
NEN 7510:2017	**A.11.2.1**	Plaatsing en bescherming van apparatuur	Ja	Ja	R & B
ISO 27001:2013	**A.11.2.2**	Nutsvoorzieningen	Ja	Ja	R & B
NEN 7510:2017	**A.11.2.2**	Nutsvoorzieningen	Ja	Ja	R & B
ISO 27001:2013	**A.11.2.3**	Beveiliging van bekabeling	Ja	Ja	C, R & B

NEN 7510:2017	**A.11.2.3**	Beveiliging van bekabeling	Nee	Nee		De dienstverlening van True omvat geen gebieden met medische apparatuur en heeft daardoor geen aanleiding tot het nemen van maatregelen om netwerk- en andere bekabeling te beschermen tegen (hoge) emissies uit medische apparaten.
ISO 27001:2013	**A.11.2.4**	Onderhoud van apparatuur	Ja	Ja	R & B	
NEN 7510:2017	**A.11.2.4**	Onderhoud van apparatuur	Nee	Nee		De dienstverlening van True omvat geen gebieden met medische apparatuur en heeft daardoor geen aanleiding tot het nemen van maatregelen om uitrusting af te schermen tegen (hoge) emissies uit medische apparaten.
ISO 27001:2013	**A.11.2.5**	Verwijdering van bedrijfsmiddelen	Ja	Ja	R & B	
NEN 7510:2017	**A.11.2.5**	Verwijdering van bedrijfsmiddelen	Ja	Ja	R & B	
ISO 27001:2013	**A.11.2.6**	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Ja	Ja	R & B	
NEN 7510:2017	**A.11.2.6**	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Nee	Nee		True kan het geautoriseerd gebruik van medische apparaten (buiten bepaalde fysieke locaties) die worden gebruikt om gegevens te registreren of te rapporteren niet garanderen. True biedt enkel garanties op de geleverde digitale infrastructuur, waarop bepaalde klantspecifieke applicaties gehost kunnen worden.
ISO 27001:2013	**A.11.2.7**	Veilig verwijderen of hergebruiken van apparatuur	Ja	Ja	R & B	
NEN 7510:2017	**A.11.2.7**	Veilig verwijderen of hergebruiken van apparatuur	Ja	Ja	R & B	
ISO 27001:2013	**A.11.2.8**	Onbeheerde gebruikersapparatuur	Ja	Ja	R & B	
NEN 7510:2017	**A.11.2.8**	Onbeheerde gebruikersapparatuur	Ja	Ja	R & B	
ISO 27001:2013	**A.11.2.9**	‘Clear desk’- en ‘clear screen’-beleid	Ja	Ja	R & B	
NEN 7510:2017	**A.11.2.9**	‘Clear desk’- en ‘clear screen’-beleid	Ja	Ja	R & B	
ISO 27001:2013	**A.12.1.1**	Gedocumenteerde bedieningsprocedures	Ja	Ja	R & B	
NEN 7510:2017	**A.12.1.1**	Gedocumenteerde bedieningsprocedures	Ja	Ja	R & B	
ISO 27001:2013	**A.12.1.2**	Wijzigingsbeheer	Ja	Ja	C, R & B	
NEN 7510:2017	**A.12.1.2**	Wijzigingsbeheer	Ja	Ja	C, R & B	

ISO 27001:2013	**A.12.1.3**	Capaciteitsbeheer	Ja	Ja	C, R & B	
NEN 7510:2017	**A.12.1.3**	Capaciteitsbeheer	Ja	Ja	C, R & B	
ISO 27001:2013	**A.12.1.4**	Scheiding van ontwikkel-, test- en productieomgevingen	Ja	Ja	R & B	
NEN 7510:2017	**A.12.1.4**	Scheiding van ontwikkel-, test- en productieomgevingen	Nee	Nee		True kan in een OTAP-straat voor klanten voorzien, maar de verantwoordelijkheid ligt bij de klant om deze OTAP-wens bij True aan te kaarten en voorwaarden te stellen aan het eigen ontwikkelproces (bijv: bij migratie van software van ontwikkelomgeving naar productie-omgeving).
ISO 27001:2013	**A.12.2.1**	Beheersmaatregelen tegen malware	Ja	Ja	C, R & B	
NEN 7510:2017	**A.12.2.1**	Beheersmaatregelen tegen malware	Ja	Ja	C, R & B	
ISO 27001:2013	**A.12.3.1**	Back-up van informatie	Ja	Ja	C, R & B	
NEN 7510:2017	**A.12.3.1**	Back-up van informatie	Ja	Ja, deels	C, R & B	
ISO 27001:2013	**A.12.4.1**	Gebeurtenissen registreren	Ja	Ja	C, R & B	
NEN 7510:2017	**A.12.4.1**	Gebeurtenissen registreren	Nee	Nee		True heeft dit ingeregeld op serverniveau en intern ontwikkelde applicaties. True kan hier echter niet in voldoende mate in voorzien voor haar zorgklanten, aangezien het in beginsel een verantwoordelijkheid is van de klant, danwel van door de klant ingehuurde externe partij, die het betreffende gezondheidsinformatiesysteem heeft ontwikkeld.
ISO 27001:2013	**A.12.4.2**	Beschermen van informatie in logbestanden	Ja	Ja	R & B	
NEN 7510:2017	**A.12.4.2**	Beschermen van informatie in logbestanden	Nee	Nee		True heeft dit ingeregeld op serverniveau en intern ontwikkelde applicaties. True kan hier echter niet in voldoende mate in voorzien voor haar zorgklanten, aangezien het in beginsel een verantwoordelijkheid is van de klant, danwel van door de klant ingehuurde externe partij, welke het betreffende gezondheidsinformatiesysteem heeft ontwikkeld.
ISO 27001:2013	**A.12.4.3**	Logbestanden van beheerders en operators	Ja	Ja	R & B	
NEN 7510:2017	**A.12.4.3**	Logbestanden van beheerders en operators	Ja	Ja	R & B	

ISO 27001:2013	**A.12.4.4**	Kloksynchronisatie	Ja	Ja	R & B
NEN 7510:2017	**A.12.4.4**	Kloksynchronisatie	Ja	Ja	R & B
ISO 27001:2013	**A.12.5.1**	Software installeren op operationele systemen	Ja	Ja	C, R & B
NEN 7510:2017	**A.12.5.1**	Software installeren op operationele systemen	Ja	Ja	C, R & B
ISO 27001:2013	**A.12.6.1**	Beheer van technische kwetsbaarheden	Ja	Ja	C, R & B
NEN 7510:2017	**A.12.6.1**	Beheer van technische kwetsbaarheden	Ja	Ja	C, R & B
ISO 27001:2013	**A.12.6.2**	Beperkingen voor het installeren van software	Ja	Ja	R & B
NEN 7510:2017	**A.12.6.2**	Beperkingen voor het installeren van software	Ja	Ja	R & B
ISO 27001:2013	**A.12.7.1**	Beheersmaatregelen betreffende audits van informatiesystemen	Ja	Ja	R & B
NEN 7510:2017	**A.12.7.1**	Beheersmaatregelen betreffende audits van informatiesystemen	Ja	Ja	R & B
ISO 27001:2013	**A.13.1.1**	Beheersmaatregelen voor netwerken	Ja	Ja	R & B
NEN 7510:2017	**A.13.1.1**	Beheersmaatregelen voor netwerken	Ja	Ja	R & B
ISO 27001:2013	**A.13.1.2**	Beveiliging van netwerkdiensten	Ja	Ja	R & B
NEN 7510:2017	**A.13.1.2**	Beveiliging van netwerkdiensten	Ja	Ja	R & B
ISO 27001:2013	**A.13.1.3**	Scheiding in netwerken	Ja	Ja	R & B
NEN 7510:2017	**A.13.1.3**	Scheiding in netwerken	Ja	Ja	R & B
ISO 27001:2013	**A.13.2.1**	Beleid en procedures voor informatietransport	Ja	Ja	R & B
NEN 7510:2017	**A.13.2.1**	Beleid en procedures voor informatietranspor	Ja	Ja	R & B
ISO 27001:2013	**A.13.2.2**	Overeenkomsten over informatietransport	Ja	Ja	C, R & B
NEN 7510:2017	**A.13.2.2**	Overeenkomsten over informatietransport	Ja	Ja	C, R & B
ISO 27001:2013	**A.13.2.3**	Elektronische berichten	Ja	Ja	R & B
NEN 7510:2017	**A.13.2.3**	Elektronische berichten	Ja	Ja	R & B
ISO 27001:2013	**A.13.2.4**	Vertrouwelijkheids- of geheimhoudingsovereenkomst	Ja	Ja	C, R & B
NEN 7510:2017	**A.13.2.4**	Vertrouwelijkheids- of geheimhoudingsovereenkomst'	Ja	Ja	C, R & B
ISO 27001:2013	**A.14.1.1**	Analyse en specificatie van informatiebeveiligingseisen	Ja	Ja	R & B

NEN 7510:2017	**A.14.1.1**	Analyse en specificatie van informatiebeveiligingseisen	Ja	Ja	R & B	
NEN 7510:2017	**A.14.1.1.1**	Zorgontvangers op unieke wijze identificeren	Nee	Nee		True ontwikkelt geen gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken. Vandaar dat True deze maatregel niet kan borgen.
NEN 7510:2017	**A.14.1.1.2**	Validatie van outputgegevens	Nee	Nee		True ontwikkelt geen gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken. Vandaar dat True deze maatregel niet kan borgen.
ISO 27001:2013	**A.14.1.2**	Toepassingen op openbare netwerken beveiligen	Ja	Ja	R & B	
NEN 7510:2017	**A.14.1.2**	Toepassingen op openbare netwerken beveiligen	Nee	Nee		De verantwoording om zorginformatie die via openbare netwerken wordt uitgewisseld, bescherming te bieden tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging ligt bij de zorgklant van True. True kan hier slechts in zeer beperkte mate ondersteuning in bieden.
ISO 27001:2013	**A.14.1.3**	Transacties van toepassingen beschermen	Ja	Ja	R & B	
NEN 7510:2017	**A.14.1.3**	Transacties van toepassingen beschermen	Ja	Ja	R & B	
NEN 7510:2017	**A.14.1.3.1**	Openbaar beschikbare gezondheidsinformatie	Nee	Nee		De verantwoordelijkheid om de integriteit van openbaar beschikbare gezondheidsinformatie te bewaken en te archiveren ligt niet bij True, maar bij de zorgklant zelf, danwel diens specifieke leverancier hieromtrent.
ISO 27001:2013	**A.14.2.1**	Beleid voor beveiligd ontwikkelen	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.1**	Beleid voor beveiligd ontwikkelen	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.2**	Procedures voor wijzigingsbeheer met betrekking tot systemen	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.2**	Procedures voor wijzigingsbeheer met betrekking tot systemen	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.3**	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.3**	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.4**	Beperkingen op wijzigingen aan softwarepakketten	Ja	Ja	R & B	

NEN 7510:2017	**A.14.2.4**	Beperkingen op wijzigingen aan softwarepakketten	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.5**	Principes voor engineering van beveiligde systemen	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.5**	Principes voor engineering van beveiligde systemen	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.6**	Beveiligde ontwikkelomgeving	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.6**	Beveiligde ontwikkelomgeving	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.7**	Uitbestede softwareontwikkeling	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.7**	Uitbestede softwareontwikkeling	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.8**	Testen van systeembeveiliging	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.8**	Testen van systeembeveiliging	Ja	Ja	R & B	
ISO 27001:2013	**A.14.2.9**	Systeemacceptatietests	Ja	Ja	R & B	
NEN 7510:2017	**A.14.2.9**	Systeemacceptatietests	Ja	Ja	R & B	
ISO 27001:2013	**A.14.3.1**	Bescherming van testgegevens	Ja	Ja	R & B	
NEN 7510:2017	**A.14.3.1**	Bescherming van testgegevens	Nee	Nee		De door True ontwikkelde applicaties zijn niet bedoeld om persoonlijke gezondheidsinformatie in te verwerken. Vandaar dat True gedurende het testproces geen aanvullende rekening behoeft te houden met testgegevens, die tot deze categorie informatie behoren.
ISO 27001:2013	**A.15.1.1**	Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja	Ja	R & B	
NEN 7510:2017	**A.15.1.1**	Informatiebeveiligingsbeleid voor leveranciersrelaties	Ja	Ja	R & B	
ISO 27001:2013	**A.15.1.2**	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Ja	Ja	R & B	
NEN 7510:2017	**A.15.1.2**	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten'	Ja	Ja	R & B	
ISO 27001:2013	**A.15.1.3**	Toeleveringsketen van informatie- en communicatietechnologie	Ja	Ja	R & B	
NEN 7510:2017	**A.15.1.3**	Toeleveringsketen van informatie- en communicatietechnologie	Ja	Ja	R & B	
ISO 27001:2013	**A.15.2.1**	Monitoring en beoordeling van dienstverlening van leveranciers	Ja	Ja	R & B	
NEN 7510:2017	**A.15.2.1**	Monitoring en beoordeling van dienstverlening van leveranciers'	Ja	Ja	R & B	
ISO 27001:2013	**A.15.2.2**	Beheer van veranderingen in dienstverlening van leveranciers	Ja	Ja	R & B	

NEN 7510:2017	**A.15.2.2**	Beheer van veranderingen in dienstverlening van leveranciers'	Ja	Ja	R & B	
ISO 27001:2013	**A.16.1.1**	Verantwoordelijkheden en procedures	Ja	Ja	C, R & B	
NEN 7510:2017	**A.16.1.1**	Verantwoordelijkheden en procedures	Ja	Ja	C, R & B	
ISO 27001:2013	**A.16.1.2**	Rapportage van informatiebeveiligingsgebeurtenissen	Ja	Ja	C, R & B	
NEN 7510:2017	**A.16.1.2**	Rapportage van informatiebeveiligingsgebeurtenissen	Ja	Ja	C, R & B	
ISO 27001:2013	**A.16.1.3**	Rapportage van zwakke plekken in de informatiebeveiliging	Ja	Ja	C, R & B	
NEN 7510:2017	**A.16.1.3**	Rapportage van zwakke plekken in de informatiebeveiliging'	Ja	Ja	C, R & B	
ISO 27001:2013	**A.16.1.4**	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Ja	Ja	C, R & B	
NEN 7510:2017	**A.16.1.4**	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen'	Ja	Ja	C, R & B	
ISO 27001:2013	**A.16.1.5**	Respons op informatiebeveiligingsincidenten	Ja	Ja	C, R & B	
NEN 7510:2017	**A.16.1.5**	Respons op informatiebeveiligingsincidenten'	Ja	Ja	C, R & B	
ISO 27001:2013	**A.16.1.6**	Lering uit informatiebeveiligingsincidenten	Ja	Ja	R & B	
NEN 7510:2017	**A.16.1.6**	Lering uit informatiebeveiligingsincidenten	Ja	Ja	R & B	
ISO 27001:2013	**A.16.1.7**	Verzamelen van bewijsmateriaal	Ja	Ja	R & B	
NEN 7510:2017	**A.16.1.7**	Verzamelen van bewijsmateriaal	Nee	Nee		True geeft geen nadere invulling aan de zorgspecifieke implementatierichtlijn, aangezien de hier in gespecificeerde bewijsvragen niet door True behandeld zouden kunnen worden.
ISO 27001:2013	**A.17.1.1**	Informatiebeveiligingscontinuïteit plannen	Ja	Ja	W, C, R & B	
NEN 7510:2017	**A.17.1.1**	Informatiebeveiligingscontinuïteit plannen	Nee	Nee		True kan geen invulling geven aan de zorgspecifieke implementatierichtlijnen, deze is voor zorgverleners. De plannen van True reiken niet verder dan de digitale omgeving welke True beheert. Dit betreft echter geen aanvulling ten opzichte van reeds genomen ISO 27001 maatregelen mbt betreffend norm-item.
ISO 27001:2013	**A.17.1.2**	Informatiebeveiligingscontinuïteit implementeren	Ja	Ja	W, C, R & B	

NEN 7510:2017	**A.17.1.2**	Informatiebeveiligingscontinuïteit implementeren	Nee	Nee		True maakt geen onderscheid in de klanten die zij bedienen bij het oplossen van continuïteitsstoringen, behoudens het afgenomen SLA niveau.
ISO 27001:2013	**A.17.1.3**	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja	Ja	W, C, R & B	
NEN 7510:2017	**A.17.1.3**	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Ja	Ja	W, C, R & B	
ISO 27001:2013	**A.17.2.1**	Beschikbaarheid van informatieverwerkende faciliteiten	Ja	Ja	C, R & B	
NEN 7510:2017	**A.17.2.1**	Beschikbaarheid van informatieverwerkende faciliteiten	Ja	Ja	C, R & B	
ISO 27001:2013	**A.18.1.1**	Vaststellen van toepasselijke wetgeving en contractuele eisen	Ja	Ja	W, C, R & B	
NEN 7510:2017	**A.18.1.1**	Vaststellen van toepasselijke wetgeving en contractuele eisen	Nee	Nee		True is geen zorginstelling en kan daardoor niet aan deze zorgspecifieke implementatierichtlijn voldoen.
ISO 27001:2013	**A.18.1.2**	Intellectuele-eigendomsrechten	Ja	Ja	W, C, R & B	
NEN 7510:2017	**A.18.1.2**	Intellectuele-eigendomsrechten	Ja	Ja	W, C, R & B	
ISO 27001:2013	**A.18.1.3**	Beschermen van registraties	Ja	Ja	W, C, R & B	
NEN 7510:2017	**A.18.1.3**	Beschermen van registraties	Ja	Ja	W, C, R & B	
ISO 27001:2013	**A.18.1.4**	Privacy en bescherming van persoonsgegevens	Ja	Ja	W, C, R & B	
NEN 7510:2017	**A.18.1.4**	Privacy en bescherming van persoonsgegevens	Nee	Nee		True kan geen invulling geven aan de zorgspecifieke implementatierichtlijnen, deze is voor de zorginstelling, danwel de aanbieder van de zorgapplicatie.
ISO 27001:2013	**A.18.1.5**	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja	Ja	W, C	
NEN 7510:2017	**A.18.1.5**	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja	Ja	W, C	
ISO 27001:2013	**A.18.2.1**	Onafhankelijke beoordeling van informatiebeveiliging	Ja	Ja	R & B	
NEN 7510:2017	**A.18.2.1**	Onafhankelijke beoordeling van informatiebeveiliging	Ja	Ja	R & B	
ISO 27001:2013	**A.18.2.2**	Naleving van beveiligingsbeleid en -normen	Ja	Ja	C, R & B	
NEN 7510:2017	**A.18.2.2**	Naleving van beveiligingsbeleid en -normen	Ja	Ja	C, R & B	
ISO 27001:2013	**A.18.2.3**	Beoordeling van technische naleving	Ja	Ja	R & B	

NEN 7510:2017	**A.18.2.3**	Beoordeling van technische naleving	Nee	Nee		True heeft geen inzicht in het kader van technische interoperabiliteit mbt de onderlinge samenwerking van gezondheidsinformatiesystemen.

Norm	Maatregel	Omschrijving maatregel	Van toepassing	Maatregel geïmplementeerd	Reden selectie	Reden uitsluiting