Verklaring van toepasselijkheid NEN7510

Norm	Omschrijving	Beheersmaatregel	Van toepassing	Geïmple-menteerd	Wet	Contract	Risico/Best practice	Onderbouwing
A.5 IB-beleid								
A.5.1 Aansturing door de directie van de IB								
Doelstelling: Het verschaffen van directieaansturing van en steun voor IB in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.								
A.5.1.1	Beleidsregels voor IB	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.	J	J			X	
A.5.1.2	Beoordelen van het IB-beleid	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.	J	J			X	
A.6 Organiseren van IB								
A.6.1 Interne organisatie								
Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de IB binnen de organisatie te initiëren en te beheersen.								

A.6.1.1	Rollen en verant-woordelijkheden IB	Organisaties moeten: 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 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.) 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.	J	J			X	
A.6.1.2	Scheiding van taken	Organisaties moeten, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden scheiden teneinde de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.	J	J			X	
A.6.1.3	Contact met overheidsinstanties	Er moeten passende contacten met relevante overheidsinstanties worden onderhouden.	J	J	X			

A.6.1.4	Contact met speciale belangengroepen	Er moeten passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden.	J	J			X	
A.6.1.5	IB in projectbeheer	Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.	J	J		X	X	
A.6.2 Mobiele apparatuur en telewerken								
Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.								
A.6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen moeten worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	J	J		X	X	
A.6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen moeten worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt bereikt, verwerkt of opgeslagen.	J	J		X	X	
A.7 Veilig personeel								
A.7.1 Voorafgaand aan het dienstverband								
Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de functies waarvoor zij in aanmerking komen.								
A.7.1.1	Screening	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.	J	J			X	

A.7.1.2	Arbeidsvoorwaarden	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.	J	J			X	
A.7.2 Tijdens het dienstverband								
Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van IB en deze nakomen.								
A.7.2.1	Directieverant-woordelijkheden	De directie moet van alle medewerkers en contractanten eisen dat ze IB toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	J	J			X	
A.7.2.2	Bewustzijn, opleiding en training ten aanzien van IB	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 moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	J	J			X	

A.7.2.3	Disciplinaire proce dure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de IB.	J	J			X	
A.7.3 Beëindiging en wijziging van dienstverband								
Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.								
A.7.3.1	Beëindiging of wijziging van verantwoordelijk-heden van het dienstverband	Verantwoordelijkhed en en taken met betrekking tot IB die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gecommuniceerd a an de medewerker of contractant, en ten uitvoer worden gebracht.	J	J			X	
A.8 Beheer van bedrijfsmiddelen								
A.8.1 Verantwoordelijkheid voor bedrijfsmiddelen								
Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.								
A.8.1.1	Inventariseren an bedrijfsmiddelen	Organisaties die persoonlijke gezondheidsinforma tie verwerken, moeten: a) verantwoording afleggen over informatiebedrijfsmi ddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen); b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmi ddelen (zie 8.1.2); c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	J	J		X	X	
A.8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden moeten een eigenaar hebben.	J	J		X	X	
A.8.1.3	Aanvaardbaar gebru ik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerken de faciliteiten moeten regels worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	J	J			X	

A.8.1.4	Teruggeven van bedrijfsmiddelen	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.	J	J			X	
A.8.2 Informatieclassificatie								
Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.								
A.8.2.1	Classificatie van informatie	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	J	J			X	
A.8.2.2	Informatie labelen	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.	J	J			X	
A.8.2.3	Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen moeten worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	J	J			X	
A.8.3 Behandelen van media								
Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.								
A.8.3.1	Beheer van verwijderbare media	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.	J	J			X	

A.8.3.2	Verwijderen van media	Alle persoonlijke gezondheidsinformatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	J	J			X	
A.8.3.3	Media fysiek overdragen	Media die informatie bevatten, moeten worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	J	J			X	
A.9 Toegangsbeveiliging								
A.9.1 Bedrijfseisen voor toegangsbeveiliging								
Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken.								

A.9.1.1	Beleid voor toegangsbeveiliging	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.	J	J			X	

A.9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers moeten alleen toegang krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	J				X	
A.9.2 Beheer van toegangsrechten van gebruikers								
Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.								
A.9.2.1	Registratie en uitschrijving van gebruikers	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.	J	J		X	X	
A.9.2.2	Gebruikers toegang verlenen	Een formele gebruikerstoegangs verleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	J	J			X	
A.9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van bevoorrechte toegangsrechten moeten worden beperkt en gecontroleerd.	J	J			X	
A.9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie moet worden beheerst via een formeel beheersproces.	J	J			X	
A.9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.	J	J			X	
A.9.2.6	Toegangsrechten intrekken of aanpassen	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.	J	J			X	

A.9.3 Gebruikersverantwoordelijkheden								
Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.								
A.9.3.1	Geheime authentica tie-informatie gebruiken	Van gebruikers moet worden verlangd dat zij zich bij het gebruiken van geheime authentic atie-informatie houden aan de praktijk van de organisatie.	J	J			X	
A.9.4 Toegangsbeveiliging van systeem en toepassing								
Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.								
A.9.4.1	Beperking toegang tot informatie	Gezondheidsinform atiesystemen die persoonlijke gezondheidsinforma tie 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 toepassingssysteme n in verband met het verwerken van persoonlijke gezondheidsinforma tie moet geïsoleerd (en gescheiden) worden van de toegang tot informatieverwerkin gsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinforma tie.	J	J			X	
A.9.4.2	Beveiligde inlogpro cedures	Indien het beleid voor toegangsbeveiliging dit vereist, moet toegang tot systemen en toepassingen worden beheerst door een beveiligde inlogprocedure.	J	J			X	
A.9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waa rborgen.	J	J			X	
A.9.4.4	Speciale systeemhul pmiddelen gebruiken	Het gebruik van systeemhulpmiddele n die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen moet worden beperkt en nauwkeurig worden gecontrole erd.	J	J			X	
A.9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncod e moet worden beperkt.	J	J			X	
A.10 Cryptografie								
A.10.1 Cryptografische beheersmaatregelen								
Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.								
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd.	J	J			X	

A.10.1.2	Sleutelbeheer	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd.	J	J			X	
A.11 Fysieke beveiliging en beveiliging van de omgeving								
A.11.1 Beveiligde gebieden								
Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatieverwerkende faciliteiten van de organisatie voorkomen.								
A.11.1.1	Fysieke beveiligingszone	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.	J	J		X	X	
A.11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden moeten worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	J	J		X	X	
A.11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en toegepast.	J	J			X	
A.11.1.4	Beschermen tegen bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken moet fysieke bescherming word en ontworpen en toegepast.	J	J		X	X	
A.11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden moeten procedures worden ontwikkeld en toegepast.	J	J		X	X	
A.11.1.6	Laad- en loslocatie	Toegangspunten zo als 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.	J	J		X	X	
A.11.2 Apparatuur								
Doelstelling: Verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.								

A.11.2.1	Plaatsing en bescherming van apparatuur	Apparatuur moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	J	J			X	
A.11.2.2	Nutsvoorzieningen	Apparatuur moet worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	J	J			X	
A.11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen interceptie, verstoring of schade.	J	J	X		X	
A.11.2.4	Onderhoud van apparatuur	Apparatuur moet correct worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	J	J			X	
A.11.2.5	Verwijdering van bedrijfsmiddelen	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.	J	J			X	
A.11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	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.)	J	J			X	

A.11.2.7	Veilig verwijderen of hergebruiken van apparatuur	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.	J	J			X	
A.11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	J	J			X	
A.11.2.9	'Clear desk'- en 'clear screen'-beleid	Er moet een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten worden ingesteld.	J	J			X	
A.12 Beveiliging bedrijfsvoering								
A.12.1 Bedieningsprocedures en verantwoordelijkheden								
Doelstelling: Correcte en veilige bediening van informatieverwerkende faciliteiten waarborgen.								
A.12.1.1	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures moeten worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	J	J			X	
A.12.1.2	Wijzigingsbeheer	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.	J	J			X	
A.12.1.3	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	J	J			X	

A.12.1.4	Scheiding van ontwikkel-, test- en productieomgevingen	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.	J	J			X	
A.12.2 Bescherming tegen malware								
Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.								
A.12.2.1	Beheersmaatregelen tegen malware	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.	J	J			X	
A.12.3 Back-up								
Doelstelling: Beschermen tegen het verlies van gegevens.								
A.12.3.1	Back-up van informatie	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.	J	J			X	
A.12.4 Verslaglegging en monitoren								
Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.								
A.12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en IB-gebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld.	J	J			X	

A.12.4.2	Beschermen van informatie in logbestanden	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.	J	J			X	
A.12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en -operators moeten worden vastgelegd en de logbestanden moeten worden beschermd en regelmatig worden beoordeeld.	J	J			X	
A.12.4.4	Kloksynchronisatie	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.	J	J			X	
A.12.5 Beheersing van operationele software								
Doelstelling: De integriteit van operationele systemen waarborgen.								
A.12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen moeten procedures worden geïmplementeerd.	J	J			X	
A.12.6 Beheer van technische kwetsbaarheden								
Doelstelling: Benutting van technische kwetsbaarheden voorkomen.								
A.12.6.1	Beheer van technische kwetsbaarheden	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	J	J		X	X	
A.12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software moeten regels worden vastgesteld en geïmplementeerd.	J	J			X	
A.12.7 Overwegingen betreffende audits van informatiesystemen								
Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.								
A.12.7.1	Beheersmaatregelen betreffende audits van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, moeten zorgvuldig worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	J	J			X	
A.13 Communicatiebeveiliging								

A.13.1 Beheer van netwerkbeveiliging								
Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatieverwerkende faciliteiten waarborgen.								
A.13.1.1	Beheersmaatregelen voor netwerken	Netwerken moeten worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	J	J			X	
A.13.1.2	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten moeten worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	J	J	X	X	X	
A.13.1.3	Scheiding in netwerken	Groepen van informatiediensten, -gebruikers en -systemen moeten in netwerken worden gescheiden.	J	J			X	
A.13.2 Informatietransport								
Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.								
A.13.2.1	Beleid en procedures voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, moeten formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht zijn.	J	J		X	X	
A.13.2.2	Overeenkomsten over informatietransport	Overeenkomsten moeten betrekking hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	J	J		X	X	
A.13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten moet passend beschermd zijn.	J	J		X	X	
A.13.2.4	Vertrouwelijkheids- of geheimhoudingsovereenkomst	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.	J	J		X	X	
A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen								
A.14.1 Beveiligingseisen voor informatiesystemen								
Doelstelling: Waarborgen dat IB integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.								

A.14.1.1	Analyse en specificatie van IB-eisen	De eisen die verband houden met IB moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	J	J		X	X	
A.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.	J	J		X	X	
A.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.	J	J		X	X	
A.14.1.2	Toepassingsdiensten op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, moet worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	J	J		X	X	
A.14.1.3	Transacties van toepassingsdiensten beschermen	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.	J	J			X	

A.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 moet worden vermeld en de integriteit ervan moet worden beschermd.	N	N				er wordt geen gebruik gemaakt van openbaar beschikbare gezondheidsinfomatie.
A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen								
Doelstelling: Bewerkstelligen dat IB wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.								
A.14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen moeten regels worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	J	J		X	X	
A.14.2.2	Procedures voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling moeten worden beheerst door het gebruik van formele controleprocedures voor wijzigingsbeheer.	J	J		X	X	
A.14.2.3	Technische beoordeling van toepassingen na wijzigingen bedieningsplatform	Als bedieningsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	J	J		X	X	
A.14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten moeten worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen moeten strikt worden gecontroleerd.	J	J		X	X	
A.14.2.5	Principes voor engineering van beveiligde systemen	Principes voor de engineering van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	J	J		X	X	

A.14.2.6	Beveiligde ontwikkelomgeving	Organisaties moeten beveiligde ontwikkelomgevingen vaststellen en passend beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	J	J		X	X	
A.14.2.7	Uitbestede software ontwikkeling	Uitbestede systeemontwikkeling moet onder supervisie staan van en worden gemonitord door de organisatie.	J	J		X	X	
A.14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten moet de beveiligingsfunctionaliteit worden getest.	J	J		X	X	
A.14.2.9	Systeemacceptatie-tests	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.	J	J		X	X	
A.14.3 Testgegevens								
Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.								
A.14.3.1	Bescherming van testgegevens	Testgegevens moeten zorgvuldig worden gekozen, beschermd en gecontroleerd.	J	J			X	
A.15 Leveranciersrelaties								
A.15.1 IB in leveranciersrelaties								
Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.								
A.15.1.1	IB-beleid voor leveranciersrelaties	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.	J	J		X	X	
A.15.1.2	Opnemen van beveiligingsaspecten in leveranciers-overeenkomsten	Alle relevante IB-eisen 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.	J	J		X	X	

A.15.1.3	Toeleveringsketen van informatie- en communicatie-technologie	Overeenkomsten met leveranciers moeten eisen bevatten die betrekking hebben op de IB-risico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	J	J	X	X	X	
A.15.2 Beheer van dienstverlening van leveranciers								
Doelstelling: Een overeengekomen niveau van IB en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.								
A.15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen.	J	J		X	X	
A.15.2.2	Beheer van veranderingen in de dienstverlening van leveranciers	Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor IB, moeten worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	J	J		X	X	
A.16 Beheer van IB-incidenten								
A.16.1 Beheer van IB-incidenten en -verbeteringen								
Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van IB-incidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.								
A.16.1.1	Verantwoordelijkheden en procedures	Directieverantwoordelijkheden en -procedures moeten worden vastgesteld om een snelle, doeltreffende en ordelijke respons op IB-incidenten te bewerkstelligen.	J	J			X	
A.16.1.2	Rapportage van IB-gebeurtenissen	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.	J	J			X	

A.16.1.3	Rapportage van zwakke plekken in de IB	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 IB registreren en rapporteren.	J	J			X	
A.16.1.4	Beoordeling van en besluitvorming over IB-gebeurtenissen	IB-gebeurtenissen moe ten worden beoordeeld en er moet worden geoordeeld of zij moeten worden geclassific eerd als IB-incidenten.	J	J			X	
A.16.1.5	Respons op IB-incidenten	Op IB-incidenten moet worden gereageerd in overeenstemming met de gedocumenteer de procedures.	J	J			X	
A.16.1.6	Lering uit IB-incidenten	Kennis die is verkregen door IB-incidenten te analyseren en op te lossen moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	J	J			X	
A.16.1.7	Verzamelen van bewijsmateriaal	De organisatie moet procedures definiëren en toepassen voor het identificeren, verza melen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	J	J			X	
A.17 IB-aspecten van bedrijfscontinuïteitsbeheer								
A.17.1 IB-continuïteit								
Doelstelling: IB-continuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.								
A.17.1.1	IB-continuïteit plannen	De organisatie moet haar eisen voor IB en voor de continuïteit van het IB-beheer in ongunstige situaties, bijv. een crisis of een ramp, vaststellen.	J	J		X	X	
A.17.1.2	IB-continuïteit implem enteren	De organisatie moet processen, procedures en beheersmaatregelen vaststellen, docum enteren, implementeren en handhaven om het vereiste niveau van continuïteit voor IB tijdens een ongunstige situatie te waarborgen.	J	J		X	X	
A.17.1.3	IB-continuïteit verifiër en, beoordelen en evalueren	De organisatie moet de ten behoeve van IB-continuïteit vastgestelde en geïmplementeer de beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	J	J		X	X	
A.17.2 Redundante componenten								
Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen.								

A.17.2.1	Beschikbaarheid van informatieverwerkende faciliteiten	Informatie verwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	J	J		X	X	
A.18 Naleving								
A.18.1 Naleving van wettelijke en contractuele eisen								
Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende IB en beveiligingseisen.								
A.18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen moeten voor elk informatiesysteem en de organisatie expliciet worden vastgesteld, gedocumenteerd en actueel gehouden.	J	J	X	X	X	
A.18.1.2	Intellectuele eigendomsrechten	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectueleeigendomsrechten en het gebruik van eigendomssoftware producten te waarborgen moeten passende procedures worden geïmplementeerd.	J	J	X	X	X	
A.18.1.3	Beschermen van registraties	Registraties moeten in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	J	J	X	X	X	
A.18.1.4	Privacy en bescherming van persoonsgegevens	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.	N	N				het verkrijgen van de toestemming van cliënten is de verantwoordelijkheid van de klanten van Calculus.
A.18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen moeten worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	J	J	X	X	X	
A.18.2 IB-beoordelingen								
Doelstelling: Verzekeren dat IB wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.								

A.18.2.1	Onafhankelijke beoordeling van IB	De aanpak van de organisatie ten aanzien van het beheer van IB en de implementatie ervan (bijv. beheersdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor IB), moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen worden beoordeeld.	J	J			X	
A.18.2.2	Naleving van beveiligingsbeleid en normen	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.	J	J			X	
A.18.2.3	Beoordeling van technische naleving	Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor IB.	J	J			X	
O.19 Privacy								
O.19.1 Hoe Calculus omgaat met privacy								
Doelstelling: Voorkomen van inbreuk op de persoonlijke levenssfeer van betrokkenen, van wie persoonsgegevens worden verwerkt.								
O.19.1.1	Privacy officer	Er is een privacy officer aangesteld, die de organisatie adviseert over de toepassing van wet- en regelgeving, de realisatie van haar doelstellingen en de wijze waarop dit gerealiseerd kan worden.	J	J	X		X	
O.19.1.2	Privacybeleid	Er is een privacybeleid, dat is ingebed in het IB management systeem.	J	J	X		X	
O.19.1.3	Verwerkersovereenkomst	Er is een verwerkersovereenkomst waarmee ook de privacyrisico's voor de klant afgedekt worden.	J	J	X	X	X	
O.19.1.4	Melding datalekken	De verwerkingsverantwoordelijke moet datalekken binnen 72 uur melden.	J	J	X	X	X	
O.19.1.5	Privacy impact assessment	Verwerkingsverantwoordelijke voert een privacy impact assessment uit bij de start van nieuwe projecten en initiatieven. Het behoort tot de zorgplicht van de verwerker om deze op te vragen om de additionele eisen aan opdrachten in kaart te hebben.	J	J	X		X	
O.19.1.6	Compliance	Reeds bestaande systemen voldoen aan de wet- en regelgeving.	J	J			X	

O.19.1.7	Privacy by design en default	Privacy by design en default wordt toegepast om de privacy kosteneffectief en duurzaam te verbeteren.	J	J			X	
O.19.1.8	Awareness	Medewerkers weten hoe de organisatie om wil gaan met privacy en handelen daar naar.	J	J			X	