A.5 Informatiebeveiligingsbeleid

A.5.1 Aansturing door de directie van de informatiebeveiliging

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging inovereenstemming met bedrijfseisen en relevante wet- en regelgeving.

A.5.1.1 Beleidsregels voor informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA[1]	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	Y	Organisaties behoren op het hoogste niveau een 'informatiebeveiligingsbeleid' te definiëren dat is goedgekeurd door de directie en dat de aanpak van de organisatie beschrijft om haar doelstellingen inzake informatiebeveiliging te bereiken. Beleidsregels inzake informatiebeveiliging behoren eisen te behandelen die voortkomen uit: a) bedrijfsstrategie; b) wet- en regelgeving en contracten; c) huidige en verwachte bedreigingen inzake informatiebeveiliging. Het informatiebeveiligingsbeleid behoort uiteenzettingen te bevatten betreffende: a) de definitie van doelstellingen en principes van informatiebeveiliging om richting te geven aan alle activiteiten die verband houden met informatiebeveiliging; b) toekenning van algemene en specifieke verantwoordelijkheden voor informatiebeveiligingsbeheer aan gedefinieerde rollen; c) processen voor het behandelen van afwijkingen en uitzonderingen. Op een lager niveau behoort het informatiebeveiligingsbeleid te worden ondersteund door onderwerpspecifieke beleidsregels die de implementatie van beheersmaatregelen inzake informatiebeveiliging verplicht stellen en die specifiek gestructureerd zijn om de behoeften van bepaalde doelgroepen binnen een organisatie aan de orde te stellen of om bepaalde onderwerpen te behandelen. Voorbeelden van dergelijke beleidsonderwerpen zijn: a) toegangsbeveiliging (zie hoofdstuk 9); b) classificatie van informatie (en verwerking) (zie 8.2); c) fysieke en omgevingsbeveiliging (zie hoofdstuk 11); d) onderwerpen die gericht zijn op de eindgebruiker zoals: 1) aanvaardbaar gebruik van bedrijfsmiddelen (zie 8.1.3.); 2) 'clear desk' en 'clear screen' (zie 11.2.9); 3) informatietransport (zie 13.2.1); 4) mobiele apparatuur en telewerken (zie 6.2); 5) beperkingen t.a.v. software-installaties en -gebruik (zie 12.6.2); e) back-up (zie 12.3); f) informatietransport (zie 13.2); g) bescherming tegen malware (zie 12.2); h) beheer van technische kwetsbaarheden (zie 12.6.1); i) cryptografische beheersmaatregelen (zie hoofdstuk 10);	Het informatiebeveiligingsbeleid behoort uiteenzettingen te bevatten over: a) de noodzaak van gezondheidsinformatiebeveiliging; b) de doelen van gezondheidsinformatiebeveiliging; c) het toepassingsgebied in verband met naleving, zoals beschreven in hoofdstuk 18; d) eisen van wet- en regelgeving en contractuele eisen, waaronder eisen met betrekking tot de bescherming van persoonlijke gezondheidsinformatie en de wettelijke en ethische verantwoordelijkheden van zorgverleners om deze informatie te beschermen; e) regelingen voor het doen van kennisgeving van informatiebeveiligingsincidenten, waaronder een kanaal waarlangs zorgen met betrekking tot vertrouwelijkheid kunnen worden geuit zonder dat men angst hoeft te hebben voor beschuldigingen of verwijten; f) het identificeren van processen en systemen die van vitaal belang zijn in de zorg ('vitaal' wil zeggen dat het falen ervan nadelige gevolgen kan hebben voor patiënten). Idealiter wordt het herzien van de inhoud van het beleid aangestuurd door de bevindingen uit de risicobeoordeling van de organisatie, hoewel in het beleid zelf alleen maar de richting hoeft te worden aangegeven, beginselen behoren te worden vermeld en naar andere documenten behoort te worden verwezen waarin de specifieke details (die vaker wijzigen) gevonden kunnen worden. Bij het opstellen van het beleidsdocument voor hun informatiebeveiliging zullen gezondheidsorganisaties met name de volgende, voor de gezondheidzorg unieke factoren, in overweging moeten nemen:

[1] SOA: Statement of Applicability (of Verklaring van toepasselijkheid)

		j) communicatiebeveiliging (zie hoofdstuk 13); k) privacy en bescherming van persoonsgegevens (zie 18.1.4); l) leveranciersrelaties (zie hoofdstuk 15). Deze beleidsregels behoren te worden gecommuniceerd aan medewerkers en relevante externe partijen in een vorm die relevant, toegankelijk en begrijpelijk is voor de beoogde lezer, bijv. in de context van een 'bewustzijns-, opleidings- en trainingsprogramma voor informatiebeveiliging' (zie 7.2.2).	g) de breedte van gezondheidsinformatie; h) de rechten en ethische verantwoordelijkheden van het personeel, zoals wettelijk overeengekomen en aanvaard door leden van beroepsorganisaties; i) de rechten van patiënten, indien van toepassing, op privacy en op inzage in hun dossier; j) de verplichtingen van clinici met betrekking tot het verkrijgen van geïnformeerde toestemming van patiënten en het handhaven van de vertrouwelijkheid van persoonlijke gezondheidsinformatie; k) de legitieme behoeften van clinici en gezondheidsorganisaties om de normale beveiligingsprotocollen opzij te kunnen zetten als zorgprioriteiten, vaak gekoppeld aan het onvermogen van bepaalde patiënten om hun voorkeuren te uiten, dit nodig maken; ook de procedures die moeten worden ingezet om dit te realiseren; l) de verplichtingen van de desbetreffende gezondheidsorganisaties en van patiënten indien zorg wordt verleend op basis van 'gedeelde zorg' of langdurige 'uitgebreide zorg'; m) de protocollen en procedures die moeten worden toegepast op het delen van informatie in het kader van onderzoek en klinische studies; n) de regelingen voor, en bevoegdheidsgrenzen van tijdelijk personeel, zoals vervangers, studenten en oproepkrachten; o) de regelingen voor en beperkingen die gesteld worden aan de toegang tot persoonlijke gezondheidsinformatie door vrijwilligers en ondersteunend personeel zoals geestelijken of personeel van charitatieve instellingen; p) de implicaties van beveiligingsmaatregelen voor de veiligheid van patiënten; q) de implicaties van informatiebeveiligingsmaatregelen voor de prestaties van gezondheidsinformatiesystemen. Veel gezondheidsorganisaties zijn tot de conclusie gekomen dat het handig is om het beleidsdocument elektronisch aan personeel ter beschikking te stellen via een informatiebeveiligingsrubriek op het intranet van de gezondheidsorganisatie.

			Scope: informatieveiligheid is niet enkel een zaak die zich beperkt tot de gezondheidsinformatie. Ook personeelsbeleid, boekhouding enz. zijn betrokken partijen. Men kan wel specifieke maatregelen uitwerken en meer focussen op de processen die enkel van toepassing zijn op de gezondheidsinformatie.

A.5.1.2 Beoordeling van hetinformatiebeveiligingsbeleid

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Y	Elk beleid behoort een eigenaar te hebben die namens de directie verantwoordelijk is voor het ontwikkelen, beoordelen en evalueren van de beleidsregels. De beoordeling behoort mede de beoordeling te omvatten van verbetermogelijkheden voor de organisatorische beleidsregels en de aanpak van het informatiebeveiligingsbeheer als antwoord op veranderingen in de omgeving van de organisatie, de bedrijfsomstandigheden, juridische voorwaarden of technische omgeving. De beoordeling van beleidsregels voor informatiebeveiliging behoort rekening te houden met de resultaten van directiebeoordelingen. Voor een herzien beleid behoort de goedkeuring van de directie te worden verkregen.	De beoordeling behoort in te gaan op: a) de veranderende aard van de bedrijfsvoering van de gezondheidsorganisatie en de gelijktijdige veranderingen voor het risicoprofiel en de risicomanagementbehoeften; b) de veranderingen die worden gedaan aan de IT-infrastructuur van de organisatie en de gelijktijdige veranderingen die deze met zich meebrengen voor het risicoprofiel van de organisatie; c) de in de externe omgeving geïdentificeerde veranderingen die op vergelijkbare wijze van invloed zijn op het risicoprofiel van de organisatie; d) de jongste beheersmaatregelen, nalevings- en zekerheidseisen en -regelingen die door de gezondheidsinstanties van een rechtsgebied of door nieuwe wet- of regelgeving verplicht worden gesteld; e) de jongste richtlijnen en aanbevelingen van organisaties van zorgverleners en van de leden van informatieprivacycommissies met betrekking tot de bescherming van persoonlijke gezondheidsinformatie; f) de resultaten van juridische casussen die bij de rechter zijn getoetst, waardoor precedenten zijn geschapen of ontkracht of waardoor 'best practices' zijn vastgesteld; g) de uitdagingen en belangrijke punten met betrekking tot het beleid, zoals aan de organisatie geuit door het personeel, patiënten en hun partners en zorgverleners, onderzoekers en overheden (bijv. leden van privacycommissies); h) rapporten over incidenten met betrekking tot de veiligheid van patiënten met als doel om deze incidenten tegen te gaan in die gevallen waarin het

			incident het gevolg is van het falen van informatiebeveiligingsmaatregelen.

A.6 Organiseren van Informatiebeveiliging

A.6.1 Interne organisatie

Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen

A.6.1.1Rollen en verantwoordelijkheden bij informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Y	Het toewijzen van de verantwoordelijkheden die bij informatiebeveiliging horen, behoort te worden gedaan in overeenstemming met de beleidsregels voor informatiebeveiliging (zie 5.1.1). Verantwoordelijkheden voor het beschermen van individuele bedrijfsmiddelen en voor het uitvoeren van specifieke informatiebeveiligingsprocessen behoren te worden geïdentificeerd. Verantwoordelijkheden behoren te worden gedefinieerd voor activiteiten met betrekking tot risicobeheer van informatiebeveiliging en in het bijzonder voor het accepteren van de overblijvende risico's. Deze verantwoordelijkheden behoren waar nodig te worden aangevuld met meer gedetailleerde richtlijnen voor specifieke locaties en informatieverwerkende faciliteiten. Lokale verantwoordelijkheden voor het beschermen van bedrijfsmiddelen en voor het uitvoeren van specifieke beveiligingsprocessen behoren te worden gedefinieerd. Personen aan wie verantwoordelijkheden inzake informatiebeveiliging zijn toegekend mogen beveiligingstaken aan anderen delegeren. Niettemin blijven zij verantwoordelijk en behoren zij vast te stellen dat gedelegeerde taken correct zijn verricht. Vastgelegd behoort te worden welke personen voor welke gebieden verantwoordelijk zijn. Het volgende behoort in het bijzonder te gebeuren: a) de bedrijfsmiddelen en informatiebeveiligingsprocessen behoren te worden geïdentificeerd en gedefinieerd; b) de entiteit die verantwoordelijk is voor elk bedrijfsmiddel of informatiebeveiligingsproces behoort te worden bepaald en de details van deze verantwoordelijkheid behoren te worden gedocumenteerd (zie 8.1.2); c) autorisatieniveaus behoren te worden gedefinieerd en gedocumenteerd; d) om in staat te zijn om de verantwoordelijkheden in het informatiebeveiligingsgebied te vervullen behoren de benoemde personen op het desbetreffende gebied competent te zijn en behoort hun de mogelijkheden te worden geboden om de ontwikkelingen bij te houden; e) coördinatie en overzicht van informatiebeveiligingsaspecten van leveranciersrelaties behoren te worden geïdentificeerd en gedocumenteerd.	*Het is belangrijk om te wijzen op de essentiële aard van managementverantwoordelijkheid in organisaties die persoonlijke gezondheidsinformatie beheren, zoals beschreven in B.2. Rekenschap en coördinatie kunnen op de lange termijn alleen worden gehandhaafd indien de organisatie over een expliciete informatiebeveiligingsbeheerinfrastructuur beschikt. Ongeacht welke organisatiestructuur wordt gekozen, is het van kritisch belang dat deze dusdanig wordt ontworpen en gestructureerd dat toegang door patiënten (bijv. om verzoeken voor het verkrijgen van persoonlijke gezondheidsinformatie in te dienen) en het rapporteren binnen de organisatiestructuur mogelijk worden gemaakt en dat de tijdige verstrekking van informatie wordt gegarandeerd.* *Zoals vermeld in B.4.3 behoort de (virtuele of daadwerkelijke) informatiebeveiligingsfunctionaris van de organisatie onder andere verslag uit te brengen aan het forum en hieraan secretariële diensten te verlenen. De functionaris behoort verantwoordelijk te zijn voor het samenstellen, publiceren en becommentariëren van de rapporten die worden ontvangen door de leden van het forum.* *Gezondheidsorganisaties behoren de uiteenzetting van het toepassingsgebied breed bekend te maken binnen de organisatie, deze vervolgens te beoordelen en te garanderen dat deze wordt overgenomen door de groepen binnen de organisatie die zich bezighouden met informatie-, klinische en corporate governance.* Bepaalde zaken horen meer toe aan de functie van de ombudsman en niet aan DPO.

			De verantwoordelijkheden en taken welke toebehoren horen aan welke functie: DPO, veiligheidsconsulent zijn wettelijk bepaald. Ombudsfunctie,… heeft geen relatie tot informatieveiligheid (is meer de busisness voor de werking van het ziekenhuis), deze functie wordt hier dus niet verder besproken. Hierboven beschreven uitleg is afkomstig uit de NEN-normen (Nederland) en de gebruikte terminologie wijkt af van de Belgische. De lokale situatie in Belgische ziekenhuizen kan dus verschillen van deze richtlijnen (die trouwens niet bindend is) Een eventueel aangepast voorstel voor de richtlijnen van deze norm moet komen van de Belgische ziekenhuizen zelf.

A.6.1.2 Scheiding van taken

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Y	Er behoort op te worden gelet dat geen enkele persoon ongemerkt of zonder autorisatie toegang kan krijgen tot bedrijfsmiddelen, ze kan wijzigen of gebruiken. Het initiëren van een gebeurtenis behoort te worden gescheiden van de autorisatie ervan. Bij het ontwerpen van beheersmaatregelen behoort rekening te worden gehouden met de mogelijkheid van samenzwering. Voor kleine organisaties kan het moeilijk zijn om taken te scheiden, maar het principe behoort te worden toegepast voor zover dit mogelijk en haalbaar is. Wanneer het moeilijk is om taken te scheiden, behoren andere beheersmaatregelen zoals het monitoren van activiteiten, audittrajecten en supervisie door de directie te worden overwogen.	

A.6.1.3 Contact met overheidsinstanties

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	N	Organisaties behoren procedures te hebben die aangeven wanneer en door wie contact behoort te worden opgenomen met overheidsinstanties (bijv. politie, regelgevende organen, toezichthouders) en hoe geïdentificeerde informatiebeveiligingsincidenten tijdig behoren te worden gerapporteerd (bijv. indien het vermoeden bestaat dat mogelijk wetgeving is overtreden).	Waarom is dit out of scope geplaatst ? Motivatie. (SOA=N) (centrale ondersteuning ?) Gaat enkel over informatieveiligheid Voorbeeld CCB, GBA,… Contacten dienen te worden onderhouden, ad-hoc, of enkel in geval van specifieke situaties (incidenten,

			rondvraag, m.b.t. ransomware, phishing, cybercriminaliteit) Kan het opstellen van protocollen nuttig zijn tussen meerdere partijen ? (vraagt veel werk, is dit wel nuttig ?) Er zijn voldoende communicatiekanalen.

A.6.1.4 Contact met speciale belangengroepen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Er behoren passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden.	N	Lidmaatschap van speciale belangengroepen of fora behoort te worden overwogen als middel om: a) kennis te verbeteren over 'best practices' en op de hoogte te blijven van relevante beveiligingsinformatie; b) ervoor te zorgen dat de kennis van informatiebeveiliging actueel en volledig is; c) vroegtijdige waarschuwingen te ontvangen inzake alarm, adviezen en patches die verband houden met aanvallen en kwetsbaarheden; d) toegang te krijgen tot gespecialiseerd advies over informatiebeveiliging; e) informatie over nieuwe technologieën, producten, bedreigingen of kwetsbaarheden te delen en uit te wisselen; f) geschikte contactpunten te verkrijgen als er informatiebeveiligingsincidenten aan de orde zijn (zie hoofdstuk 16) .	Zie hierboven, centraal ondersteund. Zelfde opmerkingen.

A.6.1.5 Informatiebeveiliging in projectbeheer

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Y	Informatiebeveiliging behoort te worden geïntegreerd in de projectbeheermethode(n) van de organisatie om ervoor te zorgen dat informatiebeveiligingsrisico's worden geïdentificeerd en aangepakt als deel van een project. Dit geldt in het algemeen voor elk project ongeacht het karakter, bijv. een project voor een proces voor kernactiviteiten, IT, 'facility management' en andere ondersteunende processen. De gebruikte projectbeheermethoden behoren te vereisen dat: a) informatiebeveiligingsdoelstellingen worden opgenomen in projectdoelstellingen; b) een risicobeoordeling van informatiebeveiliging in een vroeg stadium van het project wordt uitgevoerd om de nodige beheersmaatregelen te identificeren; c) informatiebeveiliging deel uitmaakt van alle fasen van de toegepaste projectmethodologie. In alle projecten behoren implicaties van informatiebeveiliging regelmatig te worden behandeld en beoordeeld. Verantwoordelijkheden voor informatiebeveiliging behoren te worden gedefinieerd en toegewezen aan specifieke rollen die zijn gedefinieerd in de projectbeheermethoden.	De patiëntveiligheid is een kritisch bestanddeel van de risicobeoordeling voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie. Risico's voor de veiligheid van patiënten behoren zorgvuldig te worden geanalyseerd en er behoort expliciet aandacht aan te worden besteed.

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beheren.	Y	Bij het gebruikmaken van mobiele apparatuur behoort er speciaal op te worden gelet dat bedrijfsinformatie niet wordt gecompromitteerd. Het beleid voor mobiele apparatuur behoort rekening te houden met de risico's van werken met mobiele apparatuur in onbeschermde omgevingen. Het beleid voor mobiele apparatuur behoort in overweging te nemen: a) registratie van mobiele apparatuur; b) eisen voor fysieke bescherming; c) beperking van installeren van software; d) eisen voor softwareversies voor mobiele apparatuur en voor het toepassen van patches; e) beperking van verbinding met informatiediensten; f) toegangsbeveiligingsmaatregelen; g) cryptografische technieken; h) bescherming tegen malware; i) het op afstand onbruikbaar maken, wissen, uitsluiten; j) back-ups; k) gebruik van internetdiensten en -apps. Voorzichtigheid is geboden bij het gebruik van mobiele apparatuur in openbare ruimten, vergaderruimten en andere onbeschermde locaties. Er behoort beveiliging te zijn om onbevoegde toegang tot of openbaarmaking van de op deze apparaten opgeslagen of verwerkte informatie te voorkomen, bijv. door gebruik te maken van cryptografische technieken (zie hoofdstuk 10) en het gebruik van geheime authenticatie-informatie af te dwingen (zie 9.2.4). Mobiele apparatuur behoort ook fysiek te zijn beveiligd tegen diefstal, in het bijzonder wanneer deze wordt achtergelaten in bijv. een auto of andere vervoermiddelen, in hotelkamers, conferentie- en ontmoetingscentra. Er behoort een speciale procedure te worden vastgesteld voor diefstal, verlies van mobiele apparatuur e.d. waarin rekening is gehouden met juridische, verzekerings- en andere veiligheidseisen die in de organisatie gelden. Apparatuur die belangrijke, gevoelige of essentiële bedrijfsinformatie draagt, behoort niet onbewaakt te worden achtergelaten, en behoort, waar mogelijk, fysiek achter slot en grendel te worden opgeborgen of er behoren speciale sloten te worden gebruikt om de apparatuur te beveiligen. Medewerkers die mobiele apparatuur gebruiken, behoren te worden getraind zodat ze zich bewust worden van de extra risico's die deze manier van werken met zich meebrengt en ze weten welke beheersmaatregelen behoren te worden geïmplementeerd. Als het beleid voor mobiele apparatuur toestaat dat medewerkers gebruikmaken van mobiele apparatuur die hun eigendom is, behoren het beleid en gerelateerde veiligheidsmaatregelen ook de volgende aspecten in overweging te nemen:	Organisaties behoren: a) specifiek de risico's te beoordelen die gepaard gaan met het gebruik van mobiele apparaten in de zorg; b) een beleid op te stellen inzake de voorzorgsmaatregelen die moeten worden getroffen bij het gebruik van mobiele computerapparatuur, waaronder richtlijnen en beperkingen voor het gebruik van persoonlijke apparaten binnen de organisatie, samen met beheersmaatregelen om aan de toepasselijke wettelijke privacy-eisen te voldoen; c) van hun mobiele gebruikers te eisen dat zij dit beleid volgen. Draadloze verbindingen voor mobiele netwerken kennen, hoewel deze vergelijkbaar zijn met die van bedrade netwerken, vanuit het oogpunt van informatiebeveiliging enkele belangrijke verschillen. Bepaalde draadloze versleutelingsprotocollen zoals Wired Equivalent Privacy (WEP) worden nog altijd gebruikt hoewel ze door bekende zwakheden nog maar weinig doeltreffend zijn. Bovendien worden van op mobiele apparatuur opgeslagen informatie mogelijk niet altijd back-ups gemaakt (bijv. wegens beperkte bandbreedte van het netwerk of omdat de apparatuur niet is aangesloten op de tijden waarop de back-ups zijn gepland).

		a) scheiding van privé- en zakelijk gebruik van de apparatuur, met inbegrip van het gebruik van software ter ondersteuning van een dergelijke scheiding en ter bescherming van bedrijfsgegevens op een privéapparaat; b) toegang verschaffen tot bedrijfsinformatie alleen nadat gebruikers een eindgebruikersovereenkomst hebben ondertekend waarin zij hun verplichtingen bevestigen (fysieke beveiliging, updaten van software enz.), afstand doen van eigendom van bedrijfsgegevens, toestaan dat de organisatie op afstand gegevens wist in geval van diefstal of verlies van het apparaat of indien zij niet langer geautoriseerd zijn. Dit beleid moet rekening houden met de privacywetgeving	

A.6.2.2 Telewerken

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Y	Organisaties die telewerken toestaan, behoren een beleid uit te vaardigen dat de voorwaarden en beperkingen definieert voor het telewerken. Waar van toepassing geacht en wettelijk toegestaan, behoort rekening te worden gehouden met de volgende zaken: a) de bestaande fysieke beveiliging van de telewerklocatie, waarbij rekening wordt gehouden met de fysieke beveiliging van het gebouw en de lokale omgeving; b) de voorgestelde fysieke telewerkomgeving; c) de beveiligingseisen die voor communicatie gelden, waarbij rekening wordt gehouden met de behoefte aan toegang op afstand tot de interne systemen van de organisatie, de gevoeligheid van de informatie die wordt benaderd en via de communicatiekoppeling wordt doorgegeven en de gevoeligheid van het interne systeem; d) het verlenen van virtuele desktoptoegang, waardoor het verwerken en opslaan van informatie op privéapparatuur wordt voorkomen; e) de bedreiging van onbevoegde toegang tot informatie of middelen van andere gebruikers van de accommodatie, bijv. familie en vrienden; f) het gebruik van thuisnetwerken en de eisen of beperkingen van de configuratie van draadloze netwerkdiensten; g) beleidsregels en procedures ter voorkoming van geschillen over rechten van intellectuele eigendom die is ontwikkeld op privéapparatuur; h) toegang tot privéapparatuur (om de veiligheid van het apparaat vast te stellen of tijdens een onderzoek), wat wetgeving mogelijk kan verhinderen; i) softwarelicentiecontracten waardoor de organisatie aansprakelijk kan worden gesteld voor de licenties van cliëntsoftware op werkstations die privébezit zijn van medewerkers of van externe gebruikers; j) beveiliging tegen malware en eisen aan de firewall. De in acht te nemen richtlijnen en afspraken behoren te omvatten: a) het beschikbaar stellen van passende apparatuur en opbergmeubelen voor de telewerkactiviteiten, waarbij het gebruik van privéapparatuur die niet onder het beheer van de organisatie staat, niet is toegelaten; b) een definitie van geoorloofde werkzaamheden, de werktijden, de classificatie van informatie waarover men mag beschikken en de interne systemen en diensten waartoe de telewerker bevoegde toegang heeft;	Organisaties behoren: a) beleid op te stellen inzake de voorzorgsmaatregelen die moeten worden getroffen tijdens het telewerken; b) erop toe te zien dat telewerkende gebruikers van gezondheidsinformatiesystemen zich aan dit beleid houden. Sommige nationale rechtsgebieden (bijv. in Duitsland) hebben al beperkingen gesteld aan telewerken door zorgverleners. Het is belangrijk er rekening mee te houden dat telewerken in de zorg de grenzen van rechtsgebieden kan overschrijden en zelfs kan plaatsvinden aan boord van vliegtuigen en schepen die zich buiten elk nationaal rechtsgebied bevinden. Het is mogelijk dat internationale teams die hulp verlenen bij calamiteiten, in de toekomst gebruik gaan maken van gezondheidsinformatiesystemen in andere rechtsgebieden dan die van hun thuisland. De juridische en ethische overwegingen om dit al dan niet te doen, behoren in aanmerking te worden genomen bij het ontwerpen en inzetten van gezondheidsinformatiesystemen (met name landelijke systemen) die op deze manier gebruikt kunnen worden.

		c) het beschikbaar stellen van passende communicatievoorzieningen, met inbegrip van methoden voor het beveiligen van de toegang op afstand; d) fysieke beveiliging; e) regels en richtlijnen voor toegang voor familie en bezoekers tot apparatuur en informatie; f) het beschikbaar stellen van ondersteuning en onderhoud van hardware en software; g) het regelen van de verzekering; h) de procedures voor de back-up en de bedrijfscontinuïteit; i) audit en monitoren van de beveiliging; j) intrekking van bevoegdheid en toegangsrechten, en het inleveren van apparatuur na beëindiging van de telewerkactiviteiten.	

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 rollen waarvoor zij in aanmerking komen.

A.7.1.1 Screening

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Y	Verificatie behoort rekening te houden met alle relevante wetgeving op het gebied van privacy, bescherming van persoonsgegevens en arbeidswetgeving, en behoort indien toegelaten, te omvatten: a) een verificatie () van het curriculum vitae van de sollicitant; b) bevestiging van de geclaimde academische en beroepskwalificaties; c) onafhankelijke verificatie van de identiteit (paspoort of gelijkwaardig document); d) meer gedetailleerde verificatie, zoals controle op kredietwaardigheid of strafblad indien de functie dit vereist en dit juridisch afdwingbaar is. (bv. omgaan met minderjarigen in een kinderziekenhuis) e) Worden de privacyregels cfr. GDPR – rechten van de betrokkene wel gerespecteerd ? Als een persoon wordt ingehuurd voor een specifieke informatiebeveiligingsrol, behoort de organisatie zich ervan te vergewissen dat: a) de kandidaat over de nodige competentie beschikt om de beveiligingsrol te vervullen; b) de kandidaat de rol kan worden toevertrouwd, in het bijzonder als de rol cruciaal is voor de organisatie. Als een functie, hetzij bij een eerste aanstelling, hetzij bij promotie, met zich meebrengt dat de persoon toegang heeft tot faciliteiten die informatie verwerken, en, in het bijzonder, indien het hierbij gaat om vertrouwelijke informatie, bijv. financiële informatie of zeer vertrouwelijke informatie, behoort de organisatie ook verdere, meer gedetailleerde verificaties te overwegen.	Opmerking: De toepassing van de wetgeving is eerder een juridische aangelegenheid. 'behoort indien toegelaten te omvattten': als men hier over spreekt, wat is dan –al dan niet- toegelaten? De selectieprocedure kan verschillen naar gelang het niveau of belang van een functie. Het is logisch een 'screening' voor een topfunctie te laten uitvoeren door een 'externe' 'gespecialiseerde' partij (met geheimhoudingsclausules) en neutrale ingesteldheid.

		Procedures behoren criteria en beperkingen voor controleonderzoeken te definiëren, bijv. wie is competent om personen te screenen, en hoe, wanneer en waarom worden controleonderzoeken uitgevoerd. Ook voor contractanten behoort voor een screeningprocedure te worden gezorgd. In die gevallen behoort de overeenkomst tussen de organisatie en de contractant de verantwoordelijkheden voor het uitvoeren van de screening te vermelden en de informatieprocedures die moeten worden gevolgd als de screening niet is afgemaakt of als de resultaten aanleiding geven tot twijfel of bezorgdheid. Informatie over alle kandidaten die in aanmerking komen voor posities binnen de organisatie behoort te worden verzameld en verwerkt in overeenstemming met de relevante wetgeving aanwezig in het relevante rechtsgebied. Afhankelijk van de toepasselijke wetgeving behoren kandidaten vooraf over de screeningactiviteiten te worden geïnformeerd.	

A.7.1.2 Arbeidsvoorwaarden

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Y	De contractuele verplichtingen voor medewerkers of contractanten behoren de beleidsregels van de organisatie voor informatiebeveiliging weer te geven, en tevens duidelijk te maken en te vermelden: a) dat alle medewerkers en contractanten aan wie toegang wordt verleend tot vertrouwelijke informatie een vertrouwelijkheids- of geheimhoudingsovereenkomst behoren te ondertekenen voordat hun toegang wordt verleend tot informatieverwerkende faciliteiten (zie 13.2.4); b) de wettelijke verantwoordelijkheden en rechten van de medewerker of contractant, bijv. betreffende auteursrechtwetgeving of wetgeving inzake gegevensbescherming (zie 18.1.2 en 18.1.4); c) verantwoordelijkheden voor de classificatie van informatie en het beheer van informatie van de organisatie, andere bedrijfsmiddelen die samenhangen met informatie, informatieverwerkende faciliteiten en informatiediensten die door de medewerker of contractant worden gehanteerd (zie hoofdstuk 8); d) verantwoordelijkheden van de medewerker of contractant voor het verwerken van informatie die is ontvangen van andere bedrijven of externe partijen; e) actie die moet worden ondernomen indien de medewerker of contractant de beveiligingseisen van de organisatie veronachtzaamt (zie 7.2.3). De informatiebeveiligingsrollen en de verantwoordelijkheden behoren tijdens het voortraject van het aanstellingsproces aan de kandidaten te worden gecommuniceerd. De organisatie behoort ervoor te zorgen dat medewerkers en contractanten instemmen met voorwaarden betreffende informatiebeveiliging die passen bij de aard en de mate van toegang die ze zullen krijgen tot de bedrijfsmiddelen van de organisatie die samenhangen met informatiesystemen en -diensten. Waar van toepassing behoren de verantwoordelijkheden die in de arbeidsvoorwaarden staan voor een vastgestelde periode na het einde van het dienstverband van kracht te blijven (zie 7.3).	Organisaties die persoonlijke gezondheidsinformatie verwerken behoren erop toe te zien dat werknemers of contractanten de plicht hebben schendingen van de beveiliging van gezondheidsinformatie of de privacy van patiënten te melden. In noodgevallen kan men wel proberen een ‘medewerker’ te bereiken en kan deze zijn medewerking te verlenen, afhankelijk van de ernst van de noodzaak tot tussenkomst. Specifieke ‘specialisten’ of ‘verantwoordelijken’ kunnen onder een uitzondering vallen, maar dit moet contractueel worden vastgelegd. Gezondheidsorganisaties behoren daarom aandacht te besteden aan het verzamelen van een redelijk aantal referenties en het uitvoeren van andere vormen van controle, bijv. door beroepsorganisaties en academische instellingen. Waar mogelijk zouden controles op het al dan niet bestaan van een strafblad moeten worden uitgevoerd (waar het over een wettelijke verplichting gaat) . Let wel: het is mogelijk dat deze al worden uitgevoerd in het kader van de accreditatie van zorgverleners. Zie ook 7.1.1. Zie ook ‘screening’

A.7.2 Tijdens het dienstverband

Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen

A.7.2.1 Directieverantwoordelijkheden

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	Y	De directie behoort ervoor te zorgen dat medewerkers en contractanten: a) op de juiste manier worden geïnstrueerd over hun informatiebeveiligingsrollen en verantwoordelijkheden voordat zij toegang krijgen tot vertrouwelijke informatie of informatiesystemen; b) richtlijnen ontvangen die de verwachtingen met betrekking tot hun informatiebeveiligingsrol binnen de organisatie aangeven; c) gemotiveerd zijn om te voldoen aan de beleidsregels met betrekking tot informatiebeveiliging van de organisatie; d) een niveau van bewustzijn over informatiebeveiliging bereiken dat relevant is voor hun rollen en verantwoordelijkheden binnen de organisatie (zie 7.2.2); e) zich conformeren aan de arbeidsvoorwaarden, die het informatiebeveiligingsbeleid en passende werkmethoden omvatten; f) continu beschikken over de juiste vaardigheden en kwalificaties en regelmatig worden bijgeschoold; g) via een anoniem kanaal schendingen van de beleidsregels of procedures met betrekking tot informatiebeveiliging kunnen melden (‘klokkenluider’). De directie behoort te laten zien dat ze de beleidsregels, procedures en beheersmaatregelen met betrekking tot informatiebeveiliging ondersteunt, en als rolmodel te handelen.	Het is belangrijk om te wijzen op de speciale nadruk die moet worden gelegd op de punten van zorg van patiënten die niet wensen dat hun persoonlijke gezondheidsinformatie kan worden ingezien door gezondheidswerkers die hun buren, collega's of familieleden zijn. Dergelijke punten van zorg maken een hoog percentage uit van de klachten van mensen die bevreesd zijn voor de vertrouwelijkheid van hun persoonlijke gezondheidsinformatie. Ook is het vaak zo dat personeelsleden niet onnodig in de positie willen worden geplaatst waar ze informatie over vrienden, familieleden of buren moeten beoordelen. Doeltreffend management van gezondheidsinformatiesystemen behoort op deze punten van zorg in te gaan. Zorgspecifieke implementatierichtlijnen zijn niet gericht op de Belgische situatie (algemene opmerking), kunnen deze worden geherformuleerd naar de Belgische situatie in de ziekenhuizen ?

A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	Y	Een bewustzijnsprogramma met betrekking tot informatiebeveiliging behoort erop gericht te zijn om medewerkers en, indien relevant contractanten, bewust te maken van hun verantwoordelijkheden voor informatiebeveiliging en de manieren waarop men zich van deze verantwoordelijkheden kan kwijten. Een bewustzijnsprogramma met betrekking tot informatiebeveiliging behoort te worden vastgesteld in overeenstemming met de beleidsregels en relevante procedures inzake informatiebeveiliging van de organisatie, rekening houdend met de informatie van de organisatie die moet worden beschermd en de beleidsregels die zijn geïmplementeerd om de informatie te beschermen. Het bewustzijnsprogramma behoort een aantal bewustwordingsactiviteiten te bevatten, zoals campagnes (bijv. een ‘informatiebeveiligingsdag’) en het verspreiden van boekjes of nieuwsbrieven. Bij de opzet van het bewustzijnsprogramma behoort rekening te worden gehouden met de rollen van de medewerker in de organisatie en, indien relevant, de verwachtingen van de organisatie met betrekking tot de bewustwording van contractanten. De activiteiten in het bewustwordingsprogramma behoren op zo’n manier te worden gespreid en bij voorkeur regelmatig te worden uitgevoerd dat de activiteiten worden herhaald en nieuwe medewerkers en contractanten deze ook meemaken. Het bewustwordingsprogramma behoort ook regelmatig te worden geactualiseerd, zodat het in overeenstemming blijft met	

		de beleidsregels en procedures van de organisatie, en er behoort te worden voortgebouwd op de lessen die zijn geleerd uit informatiebeveiligingsincidenten. Bewustzijnstraining behoort te worden uitgevoerd zoals vereist door het bewustzijnsprogramma inzake informatiebeveiliging van de organisatie. Bewustzijnstraining kan op verschillende manieren worden gevolgd, bijv. klassikaal, via afstandsonderwijs, via internet, in eigen tempo. Opleiding en training met betrekking tot informatiebeveiliging behoren ook algemene aspecten te omvatten zoals: a) het aangeven van de betrokkenheid van de directie bij informatiebeveiliging in de gehele organisatie; b) de noodzaak om bekend te worden met en te voldoen aan de van toepassing zijnde regels en verplichtingen met betrekking tot informatiebeveiliging zoals gedefinieerd in beleidsregels, normen, wetten, regelgeving, contracten en overeenkomsten; c) persoonlijke verantwoordelijkheid voor eigen doen en laten, en algemene verantwoordelijkheden ten opzichte van het beveiligen of beschermen van informatie die eigendom is van de organisatie en externe partijen; d) basisprocedures inzake informatiebeveiliging (zoals het melden van informatiebeveiligingsincidenten) en basisbeheersmaatregelen (zoals wachtwoordbeveiliging, malwarecontroles en opgeruimde bureaus); e) contactpunten en bronnen voor aanvullende informatie en advies over informatiebeveiligingsaangelegenheden, met inbegrip van aanvullend opleidings- en trainingsmateriaal met betrekking tot informatiebeveiliging. Opleiding en training voor informatiebeveiliging behoort periodiek plaats te vinden. De basisopleiding en -training geldt voor personen die worden overgeplaatst naar nieuwe functies of rollen met substantieel verschillende eisen ten aanzien van informatiebeveiliging, niet alleen voor nieuwe starters, en behoort plaats te vinden voordat de rol actief wordt. De organisatie behoort het opleidings- en trainingsprogramma te ontwikkelen om de opleiding en training doeltreffend uit te kunnen voeren. Het programma behoort in overeenstemming te zijn met de beleidsregels en relevante procedures inzake informatiebeveiliging van de organisatie, rekening houdend met de informatie van de organisatie die moet worden beschermd en de beleidsmaatregelen die zijn geïmplementeerd om de informatie te beschermen. Het programma behoort verschillende vormen van opleiding en training te bevatten, bijv. lezingen of zelfstudie.	

A.7.2.3 Disciplinaire procedure

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Y	De disciplinaire procedure behoort niet te worden gestart voordat is geverifieerd dat een inbreuk op de informatiebeveiliging heeft plaatsgevonden (zie 16.1.7). De formele disciplinaire procedure behoort te waarborgen dat medewerkers die worden verdacht van een inbreuk op de informatiebeveiliging correct en eerlijk worden behandeld. De formele disciplinaire procedure behoort te voorzien in een gegradueerd antwoord dat rekening houdt met factoren zoals de aard en ernst van de inbreuk en de impact ervan op de bedrijfsvoering, of dit een eerste of herhaalde overtreding is, of de overtreder al dan niet juist getraind was, relevante wetgeving, zakelijke contracten en, indien vereist, andere factoren.	De disciplinaire processen van gezondheidsorganisaties met betrekking tot schendingen van informatiebeveiliging behoren procedures te volgen die in beleid worden weerspiegeld en daarom bekend zijn bij de persoon of personen waarop het disciplinaire proces van toepassing is. In aanvulling op het voldoen aan de wetgeving die van toepassing is, behoren dergelijke processen te voldoen aan de afspraken die

		De disciplinaire procedure behoort ook te worden gebruikt als een afschrikmiddel om te voorkomen dat medewerkers de beleidsregels en procedures met betrekking tot informatiebeveiliging overtreden en om eventuele andere inbreuken op de informatiebeveiliging te voorkomen. Bij opzettelijke inbreuken kan onmiddellijke actie vereist zijn.	zijn gemaakt tussen zorgverleners en de organisaties van zorgverleners.

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 verantwoordelijkheden van het dienstverband

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	Y	Tot het communiceren van verantwoordelijkheden na beëindiging van het dienstverband behoren voortdurende eisen en wettelijke verantwoordelijkheden met betrekking tot informatiebeveiliging en, waar van toepassing, verantwoordelijkheden die zijn opgenomen in vertrouwelijkheidsovereenkomsten (zie 13.2.4) en de arbeidsvoorwaarden (zie 7.1.2) die gedurende een gedefinieerde periode na beëindiging van het dienstverband van de medewerker of contractant van kracht blijven. Verantwoordelijkheden en plichten die van kracht blijven na beëindiging van het dienstverband behoren te worden opgenomen in de arbeidsvoorwaarden van de medewerker of contractant (zie 7.1.2). Wijzigingen in verantwoordelijkheid of dienstverband behoren te worden gemanaged als het beëindigen van de desbetreffende verantwoordelijkheid of het desbetreffende dienstverband behoort te worden gecombineerd met het initiëren van de nieuwe verantwoordelijkheid of het nieuwe dienstverband.	Het is belangrijk om op te merken dat het in de zorg gebruikelijk is dat allerlei verschillende types personeel, bijv. artsen en verplegend personeel, trainingsprogramma's en andere 'afwisselingen' doorlopen waarbij hun toegangsrechten fundamenteel kunnen veranderen. Om te garanderen dat eerdere rechten worden beëindigd die niet langer vereist zijn voor hun rol, behoren dergelijke veranderingen in de werkkring in eerste instantie op dezelfde manier te worden verwerkt als het geval is bij personen waarvan het dienstverband bij de organisatie eindigt.

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 van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.	Y	Een organisatie behoort bedrijfsmiddelen die relevant zijn in de levenscyclus van informatie te identificeren en hun belang te documenteren. De levenscyclus van informatie behoort aanmaak, verwerking, opslag, overdracht, verwijdering en vernietiging te omvatten. Documentatie behoort te worden onderhouden in speciale of bestaande inventarislijsten indien van toepassing. De inventarislijst van de bedrijfsmiddelen behoort nauwkeurig, actueel, consistent en in overeenstemming met andere inventarisoverzichten te zijn. Voor elk van de geïdentificeerde bedrijfsmiddelen behoort het eigenaarschap te worden toegekend (zie 8.1.2) en de classificatie te worden geïdentificeerd (zie 8.2).	Organisaties die gezondheidsinformatie verwerken, behoren regels te hebben voor het actueel houden van informatiebedrijfsmiddelen (bijv. een medicijnendatabase) en het handhaven van de integriteit van deze bedrijfsmiddelen (bijv. de functionele integriteit van medische apparaten die worden gebruikt om gegevens te registreren of rapporteren). Medische apparaten die worden gebruikt om gegevens te registreren of rapporteren (bv. MRI) kunnen speciale

			beveiligingsoverwegingen vereisen met betrekking tot de omgeving waarin ze worden gebruikt en de elektromagnetische emissies die tijdens het gebruik ervan plaatsvinden. Dergelijke apparaten behoren op unieke wijze te worden geïdentificeerd. Er dient beschreven te worden op welke drager de (medische) informatie opgeslagen is. (vast,mobiel,toegankelijk via netwerk,..) en op welke wijze deze worden beveiligd. Opmerking: Informatie zelf is ook een bedrijfsmiddel en moet aldus ook worden geïnventariseerd.

A.8.1.2 Eigendom van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	Y	Personen evenals andere entiteiten die een door de directie goedgekeurde verantwoordelijkheid hebben voor de levenscyclus van een bedrijfsmiddel, komen in aanmerking om te worden benoemd als eigenaar van een bedrijfsmiddel. Gewoonlijk wordt een procedure geïmplementeerd die ervoor zorgt dat de benoeming van de eigenaar van bedrijfsmiddelen tijdig plaatsvindt. Het eigenaarschap behoort te worden toegekend als bedrijfsmiddelen worden aangemaakt of als bedrijfsmiddelen naar de organisatie worden overgebracht. De eigenaar van het bedrijfsmiddel behoort verantwoordelijk te zijn voor het juiste beheer ervan voor de gehele levenscyclus van het bedrijfsmiddel. De eigenaar van het bedrijfsmiddel behoort: a) ervoor te zorgen dat bedrijfsmiddelen worden geïnventariseerd; b) ervoor te zorgen dat bedrijfsmiddelen passend worden geclassificeerd en beschermd; c) toegangsbeperkingen en classificatie van belangrijke bedrijfsmiddelen te definiëren en periodiek te beoordelen, rekening houdend met de van toepassing zijnde beleidsregels voor toegangsbeveiliging; d) te zorgen voor een juiste gang van zaken als het bedrijfsmiddel wordt verwijderd of vernietigd. e)	Het is belangrijk om op te merken dat, hoewel veel informatiebedrijfsmiddelen eigendom kunnen zijn in de conventionele betekenis, er aan het concept van eigendom van persoonlijke gezondheidsinformatie allerlei juridische, ethische en op beleid gebaseerde aspecten kleven. In veel rechtsgebieden kunnen individuen rechten hebben met betrekking tot hun eigen persoonlijke gezondheidsinformatie die elk simpel concept van 'eigendom' van deze informatie van een zorginstelling of een zorgverlener beperken of overstijgen. Het is eerder zo dat zorginstellingen en zorgverleners met betrekking tot persoonlijke gezondheidsinformatie vaak als beheerders of bewaarders worden gezien.

A.8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Y	Medewerkers en externe gebruikers die bedrijfsmiddelen van de organisatie gebruiken of er toegang toe hebben, behoren bewust te worden gemaakt van de informatiebeveiligingseisen van de informatie van de organisatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten en bronnen. Zij behoren verantwoordelijk te zijn voor hun gebruik van informatievoorzieningen en voor gebruik onder hun verantwoordelijkheid.	

A.8.1.4 Teruggeven van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben, bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	Y	In de beëindigingsprocedure behoort formeel het teruggeven van alle eerder verstrekte fysieke en elektronische bedrijfsmiddelen die het eigendom zijn van of toevertrouwd zijn aan de organisatie te worden opgenomen. Ingeval een medewerker of een gebruiker van een externe partij apparatuur van de organisatie koopt of eigen persoonlijke apparatuur gebruikt, behoren procedures te worden gevolgd om ervoor te zorgen dat alle relevante informatie aan de organisatie wordt overgedragen en nauwkeurig van de apparatuur wordt verwijderd (zie 11.2.7). Ingeval een medewerker of externe gebruiker beschikt over kennis die belangrijk is voor de lopende bedrijfsvoering, behoort die informatie te worden gedocumenteerd en aan de organisatie te worden overgedragen. Tijdens de opzegtermijn behoort de organisatie controle uit te oefenen op onbevoegd kopiëren van relevante informatie (bijv. intellectuele eigendom) door medewerkers en contractanten van wie het dienstverband is opgezegd.	

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	Y	Classificaties en de bijbehorende beschermende beheersmaatregelen voor informatie behoren rekening te houden met de zakelijke behoeften om informatie te delen of te beperken, en met wettelijke eisen. Andere bedrijfsmiddelen dan informatie kunnen ook worden geclassificeerd in overeenstemming met de classificatie van informatie die is opgeslagen in, verwerkt door of anderszins behandeld of beschermd door het bedrijfsmiddel. Eigenaren van informatiebedrijfsmiddelen behoren verantwoordelijk te zijn voor de classificatie ervan. Het classificatieschema behoort regels voor het classificeren te bevatten en criteria voor het na verloop van tijd opnieuw beoordelen van de classificatie. Het beschermingsniveau dat in het schema wordt vastgelegd, behoort te worden vastgesteld door de vertrouwelijkheid, integriteit en beschikbaarheid en eventuele andere eisen voor de desbetreffende informatie te analyseren. Het schema behoort in overeenstemming te worden gebracht met het beleid voor toegangsbeveiliging (zie 9.1.1). Elk niveau behoort een naam te krijgen die betekenis heeft in de context van de toepassing van het classificatieschema. Het schema behoort organisatiebreed consistent te zijn zodat iedereen informatie en gerelateerde bedrijfsmiddelen op dezelfde manier classificeert op basis van een gemeenschappelijk begrip van beschermingseisen en de passende bescherming toepast. Classificatie behoort te worden opgenomen in de procedures van de organisatie en organisatiebreed consistent en coherent te zijn. Resultaten van classificatie behoren de waarde van bedrijfsmiddelen aan te geven afhankelijk van hun gevoeligheid en belang voor de organisatie, bijv. in de zin van vertrouwelijkheid, integriteit en beschikbaarheid.	Het vaststellen van beschermingsniveaus voor informatiebedrijfsmiddelen in de zorg is complex en vergelijkingen met classificaties van overheids- of militaire gegevens kunnen misleidend zijn. De volgende kenmerken zijn belangrijke kenmerken van informatiebedrijfsmiddelen binnen de zorg. a) De vertrouwelijkheid van persoonlijke gezondheidsinformatie is vaak grotendeels eerder subjectief dan objectief. Met andere woorden: uiteindelijk kan alleen de persoon waarop de gegevens betrekking hebben (d.w.z. de patiënt) goed de relatieve vertrouwelijkheid bepalen van verschillende gegevensvelden of -groeperingen. Een persoon die een relatie waarin hij of zij werd mishandeld, is ontvlucht, zal het veel belangrijker vinden dat zijn of haar nieuwe adres en telefoonnummer geheim wordt gehouden dan klinische gegevens over het zetten van zijn of haar gebroken arm. b) De vertrouwelijkheid van persoonlijke gezondheidsinformatie is contextafhankelijk. Zo is het bijvoorbeeld mogelijk dat een patiënt zijn naam en adres op een lijst van mensen die zijn

		Resultaten van classificatie behoren te worden geactualiseerd in overeenstemming met wijzigingen in hun waarde, gevoeligheid en belang in de loop van hun levenscyclus. Voorstel tot classificatieschema opstellen: welke soorten classificatie (bv. publiek, intern, medisch,..); er dient ermee rekening te worden gehouden dat sommige ziekenhuizen al een eigen classificatiesysteem gebruiken (bv. Vertrouwelijk, niet- vertrouwelijk..) Het lijkt onwaarschijnlijk dat alle ziekenhuizen zomaar hetzelfde systeem zullen implementeren, maar men moet streven naar een zekere compabiliteit m.b.t. uitwisseling van informatie. Dit moet onderling worden overlegd. Voorstel of voorbeeld ter inspiratie: de minimale normen van de sociale zekerheid https://www.ksz-bcss.fgov.be/sites/default/files/assets/gegevensbescherming/bld_data_data_classificatie.pdf	binnengekomen op de eerste hulp van een ziekenhuis, niet als direct vertrouwelijk beschouwt, terwijl dezelfde naam en hetzelfde adres op een lijst van mensen die zijn opgenomen in een kliniek waar mensen die aan seksuele impotentie lijden worden behandeld, door die persoon als zeer vertrouwelijk wordt beschouwd. c) De vertrouwelijkheid van persoonlijke gezondheidsinformatie kan gedurende de levensduur van het medische dossier van een individu verschuiven. Zo hebben de veranderende maatschappelijke attitudes gedurende de afgelopen 20 jaar ertoe geleid dat veel patiënten hun seksuele geaardheid niet langer als vertrouwelijk beschouwen. De houdingen ten opzichte van drugs- en alcoholverslaving hebben er daarentegen toe geleid dat bepaalde patiënten gegevens over verslavingszorg nu als nog vertrouwelijker beschouwen dan ze 20 jaar geleden zouden hebben gedaan. Omdat men niet kan voorspellen hoe gevoelig een bepaald element van persoonlijke gezondheidsinformatie is met betrekking tot alle toepassingen en alle fasen van de levenscyclus van dat element, behoort alle persoonlijke gezondheidsinformatie altijd op de juiste zorgvuldige wijze te worden beschermd. Let op: hoewel alle persoonlijke gezondheidsinformatie op uniforme wijze als vertrouwelijk behoort te worden geclassificeerd, kunnen praktische overwegingen het nodig maken de dossiers te identificeren van die patiënten waarvoor er een verhoogd risico kan bestaan dat mensen die geen noodzaak tot kennisneming hebben, er toegang toe hebben. Dergelijke individuen zijn onder andere werknemers van de organisatie op zich (met name als hun conditie emotionele gedragingen oproept), regeringsleiders, beroemdheden, politici, nieuwsmakers en leden van groepen die uitzonderlijk hoge risico's lopen (bijv. mensen met een seksueel overdraagbare aandoening of mensen van wie de persoonlijke gezondheidsinformatie informatie bevat over genetische aanleg voor een ernstige ziekte). Het kan nodig zijn de dossiers van zulke individuen van een speciaal label te voorzien zodat de toegang ertoe nauwgezet kan worden gemonitord. Het implementeren van dergelijke regelingen behoort echter met de nodige

			zorg te gebeuren, aangezien dit labelen het probleem dat men ermee wil vermijden juist kan verergeren, d.w.z. dat het de aandacht juist kan vestigen op de gelabelde gegevens. Het is ook belangrijk te benadrukken dat waar bepaalde patiënten een verhoogd risico kunnen lopen, hun persoonlijke gezondheidsinformatie niet per definitie meer vertrouwelijk is dan die van andere patiënten. *Alle* persoonlijke gezondheidsinformatie is vertrouwelijk en behoort ook zo te worden behandeld. Zie ook de bespreking onder de zorgspecifieke implementatierichtlijn in 7.2.1. Het als vertrouwelijk identificeren en (waar van toepassing) uit beschermingsoogpunt labelen van informatiebedrijfsmiddelen kan een belangrijk instrument zijn bij het trainen van personeel en bij de naleving van het beleid. Dit werkt het beste als de classificatie als een indicator van vereiste praktijken voor het hanteren van informatie fungeert. De classificatie kan ook een belangrijk bestanddeel zijn van overeenkomsten over gegevensbescherming tussen rechtsgebieden en met derde-organisaties en het personeel van die organisaties. Het identificeren en labelen van informatiebedrijfsmiddelen is ook een essentieel bestanddeel van ISO/IEC 27002. In aanvulling op de traditionele classificatie van gegevens op basis van hoe gevoelig ze zijn voor openbaarmaking, is het ook nodig de kritikaliteit te classificeren van informatie, d.w.z. de mate waarin de beschikbaarheid en integriteit van de informatie essentieel zijn voor de voortdurende verlening van zorg. Tijdsfactoren die betrokken zijn bij klinische processen, spelen vaak een cruciale rol bij het vaststellen van de beschikbaarheidseisen voor persoonlijke gezondheidsinformatie. Classificatie met betrekking tot beschikbaarheid, integriteit en kritikaliteit behoort ook te worden toegepast op processen, IT-apparaten, software, locaties en personeel. Kritikaliteit behoort via een risicobeoordeling te worden geïdentificeerd. Voorstel tot classificatieschema opstellen: welke soorten classificatie (bv. publiek, intern,medisch,..); er dient ermee rekening te worden gehouden dat sommige ziekenhuizen al een eigen classificatiesysteem gebruiken (bv. vertrouwelijk, niet- vertrouwelijk.)

			Het lijkt onwaarschijnlijk dat alle ziekenhuizen zomaar hetzelfde systeem zullem implementeren, maar men moet streven naar een zekere compabiliteit voor de onderlinge uitwisseling van gegevens. BV. een 'medisch' gegeven kan niet zo maar 'publiek' worden na overdracht. Opmerking: de classificatie moet in het verwerkingsregister van de processen in het kader van de GDPR (AVG) worden ingeschreven en gekoppeld worden aan de retentietijd voor de data.

A.8.2.2 Informatie labelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Y	Procedures voor het labelen van informatie behoren te gaan over informatie en gerelateerde bedrijfsmiddelen in fysieke en elektronische formaten. De labeling behoort in overeenstemming te zijn met het classificatieschema vastgesteld in 8.2.1. De labels behoren gemakkelijk herkenbaar te zijn. De procedures behoren richtlijnen te geven over waar en hoe labels zijn bevestigd, rekening houdend met hoe de informatie wordt bereikt of hoe de bedrijfsmiddelen worden gehanteerd afhankelijk van de soorten media. De procedures kunnen gevallen definiëren waarin labelen niet wordt toegepast, bijv. bij niet-vertrouwelijke informatie, om de werklast te verminderen. Medewerkers en contractanten behoren op de hoogte te worden gebracht van de labelprocedures. Output van systemen die informatie bevatten die is geclassificeerd als gevoelig of essentieel behoort een passend classificatielabel te dragen.	Niet alle gezondheidsinformatie is vertrouwelijk en niet alle gezondheidsinformatiesystemen bieden gebruikers toegang tot persoonlijke gezondheidsinformatie. Gebruikers van gezondheidsinformatiesystemen behoren het te weten als de gegevens waartoe zij zich toegang verschaffen persoonlijke gezondheidsinformatie bevatten. Labelen lijkt eenvoudig op fysische dragers zoals klassieke classeurs, maar hoe moet men dit implementeren op digitale gegevens. Is dit niet eerder een deel van het authentificatie- en toegankelijkheidsproces ? Wie beslist over toegang tot specifieke classificatieniveaus ? Wie kan dit onderhouden ?

A.8.2.3 Behandelen van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Y	Voor het hanteren, verwerken, opslaan en communiceren van informatie behoren procedures te worden opgesteld die consistent zijn met de classificatie van de informatie (zie 8.2.1). Met de volgende aspecten behoort rekening te worden gehouden: a) toegangsbeperkingen die de beschermingseisen van elk classificatieniveau ondersteunen; b) onderhoud van een formele verslaglegging van de bevoegde ontvangers van bedrijfsmiddelen;	

		c) bescherming van tijdelijke of permanente kopieën van de informatie tot een niveau dat consistent is met de bescherming van de originele informatie; d) opslag van IT-bedrijfsmiddelen in overeenstemming met de voorschriften van de fabrikant; e) duidelijke markering van alle kopieën van media ter attentie van de bevoegde ontvanger. Het binnen de organisatie gebruikte classificatieschema is mogelijk niet gelijk aan de schema's die door andere organisaties worden gebruikt, zelfs als de namen van de niveaus gelijk zijn; bovendien kan informatie die zich tussen organisaties beweegt variëren in classificatie afhankelijk van de context in elke organisatie, zelfs als de classificatieschema's identiek zijn. Overeenkomsten met andere organisaties waar het delen van informatie in voorkomt, behoren procedures te bevatten voor het identificeren van de classificatie van die informatie en voor het interpreteren van de classificatielabels van andere organisaties.	

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	Y	Voor het beheren van verwijderbare media behoren de volgende richtlijnen in acht te worden genomen: a) van herbruikbare media die de organisatie verlaten, behoort de inhoud, als die niet meer nodig is, onherstelbaar te worden verwijderd; b) indien nodig en haalbaar behoort goedkeuring te worden verkregen om media uit de organisatie te verwijderen en er behoort een verslaglegging van dergelijke verwijderingen te worden bijgehouden voor het onderhouden van een audittraject; c) alle media behoren te worden opgeslagen in een veilige beveiligde omgeving, in overeenstemming met de voorschriften van de fabrikant; d) indien vertrouwelijkheid of integriteit van gegevens belangrijke overwegingen zijn, behoren cryptografische technieken te worden gebruikt om gegevens op verwijderbare media te beschermen; e) om het risico te verkleinen dat media in kwaliteit achteruitgaan terwijl de opgeslagen gegevens nog nodig zijn, behoren de gegevens te worden overgebracht naar nieuwe media voordat ze onleesbaar worden; f) van waardevolle gegevens behoren meerdere kopieën op verschillende media te worden opgeslagen om het risico verder te verminderen van toevallige beschadiging of verlies van gegevens; g) om de kans op verlies van gegevens te beperken behoort registratie van verwijderbare media te worden overwogen; h) stations voor verwijderbare media behoren alleen te worden vrijgegeven als er een bedrijfsreden is om dit te doen; i) als er behoefte is om verwijderbare media te gebruiken behoort de overdracht van informatie op dergelijke media te worden gemonitord.	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te garanderen dat alle persoonlijke gezondheidsinformatie die op verwijderbare media wordt opgeslagen: a) versleuteld wordt tijdens de overdracht van de desbetreffende media of b) beschermd wordt tegen diefstal tijdens de overdracht van de desbetreffende media. c) Een beschrijving van de legitieme retentietijden moet worden uitgewerkt adhv bestaande reglementeringen en gedocumenteerd in het verwerkingsregister bij de classificatieschema's. Deze indeling met worden goedgekeurd door het management van de instelling, met juridische ondersteuning.

		j) Procedures en autorisatieniveaus behoren te worden gedocumenteerd.	

A.8.3.2 Verwijderen van media

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Y	Voor het beveiligd verwijderen van media behoren formele procedures te worden vastgesteld om het risico zo klein mogelijk te houden dat vertrouwelijke informatie bij onbevoegde personen terechtkomt. De procedures voor het beveiligd verwijderen van media die vertrouwelijke informatie bevatten, behoren in verhouding te staan tot de gevoeligheid van die informatie. Met de volgende aspecten behoort rekening te worden gehouden: a) media die vertrouwelijke informatie bevatten behoren op een beveiligde manier te worden opgeslagen en verwijderd, bijv. door verbranding of versnippering, of de gegevens behoren te worden gewist voordat de media worden gebruikt door een andere toepassing in de organisatie. b) er behoren procedures te zijn om media te identificeren die mogelijk veilig moeten worden verwijderd; c) mogelijk is het eenvoudiger om ervoor te kiezen alle media in te zamelen en veilig te verwijderen in plaats van te proberen de gevoelige media te scheiden van de rest; d) veel organisaties bieden voor media inzamelings- en verwijderingsdiensten aan; de keuze voor een passende externe partij die beschikt over adequate beheersmaatregelen en ervaring behoort zorgvuldig te gebeuren; e) verwijdering van gevoelige media behoort te worden geregistreerd om een audittraject te onderhouden. Bij het accumuleren van media voor verwijdering behoort rekening te worden gehouden met het aggregatie-effect, waardoor een grote hoeveelheid niet-gevoelige informatie gevoelig kan worden.	Het niet op de juiste wijze verwijderen van media blijft een bron van ernstige schendingen van de vertrouwelijkheid van patiënten. Het is met name belangrijk op te merken dat deze beheersmaatregel behoort te worden toegepast voordat eventuele betreffende uitrusting wordt hersteld of verwijderd. Deze eis is ook van toepassing op medische apparaten die worden gebruikt om gegevens te registreren of rapporteren. Er dient voor de verschillende apparatuur bekeken te worden wat de juiste wijze is om gegevens correct te verwijderen zodat ze niet toegankelijk worden door ‘derden’.

A.8.3.3 Media fysiek overdragen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Y	De volgende richtlijnen behoren te worden overwogen om media die informatie bevatten te beschermen tijdens transport: a) er behoren betrouwbare transport- of koeriersdiensten te worden gebruikt; b) met de directie kan worden afgesproken welke koeriersdiensten bevoegd zijn; c) er behoren procedures te worden ontwikkeld om de identificatie van koeriers te verifiëren; d) de verpakking behoort toereikend te zijn om de inhoud te beschermen tegen fysieke schade die tijdens transport kan ontstaan en behoort in overeenstemming te zijn met de voorschriften van de fabrikant, bijv. bescherming tegen milieufactoren die het herstelvermogen van de media kunnen verminderen zoals blootstelling aan hitte, vocht of elektromagnetische velden; e) er behoren registraties te worden bijgehouden die de inhoud van de media en de toegepaste bescherming identificeren en waarin wordt vastgelegd hoe vaak de media zijn vervoerd naar de beheerder en het in ontvangst nemen op de plaats van bestemming.	

A.9 Toegangsbeveiliging

A.9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: Toegang tot informatie en informatieverwerkende faciliteiten beperken

A.9.1.1 Beleid voor toegangsbeveiliging

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Y	Eigenaren van bedrijfsmiddelen behoren passende regels voor toegangsbeveiliging, -rechten en -beperkingen voor specifieke gebruikersrollen ten aanzien van hun bedrijfsmiddelen vast te stellen, waarbij de details en de striktheid van de beheersmaatregelen een afspiegeling zijn van de gerelateerde informatiebeveiligingsrisico's. Toegangsbeveiligingsmaatregelen zijn zowel logisch als fysiek van aard (zie hoofdstuk 11) en behoren als een geheel te worden beschouwd. Gebruikers en dienstverleners behoren een duidelijke verklaring te ontvangen waarin is vastgelegd aan welke bedrijfseisen de toegangsbeveiligingsmaatregelen moeten voldoen. Het beleid behoort rekening te houden met het volgende: a) beveiligingseisen van de bedrijfstoepassingen; b) beleidsregels voor informatieverspreiding en -autorisatie, bijv. het 'need-to-know'-principe, informatiebeveiligingsniveaus en -classificatie (zie 8.2); c) consistentie tussen de toegangsrechten en de beleidsregels inzake informatieclassificatie van systemen en netwerken; d) relevante wetgeving en contractuele verplichtingen met betrekking tot beperking aan de toegang tot gegevens of diensten (zie 18.1); e) het beheer van toegangsrechten in een distributie- en netwerkomgeving die alle beschikbare soorten verbindingen herkent; f) scheiding van toegangsbeveiligingsrollen, bijv. toegangsverzoek, -autorisatie, -administratie; g) eisen voor formele autorisatie van toegangsverzoeken (zie 9.2.1 en 9.2.2); h) eisen voor het periodiek beoordelen van toegangsrechten (zie 9.2.5); i) intrekken van toegangsrechten (zie 9.2.6); j) archiveren van verslaglegging van alle belangrijke gebeurtenissen betreffende het gebruik en het beheer van gebruikersidentificaties en geheime authenticatie-informatie; k) rollen met speciale toegangsrechten (zie 9.2.3).	Het is belangrijk om op te merken dat, om te voorkomen dat de verlening van zorg vertraagd wordt of stokt, er krachtigere eisen dan gebruikelijk voor een duidelijk beleid en proces, met bijbehorende autorisatie, gelden om de 'normale' toegangscontroleregels in noodsituaties te omzeilen. Gezondheidsorganisaties worden ertoe opgeroepen de implementatie van een gefedereerde identiteits- en toegangsmanagementoplossing in overweging te nemen met het oog op de mogelijke aanvullende ondersteuning en lagere beheerkosten die zo'n oplossing voor het toegangscontrolebeleid zal opleveren. Bovendien zal dit beveiligingstoegangsprocessen op hoger niveau, zoals op smartcards gebaseerde toegang en 'single sign-on'-functionaliteit, ondersteunen. Aanvullende richtlijnen over toegangscontrole in zorggerelateerde toepassingen zijn te vinden in ISO 22600.

A.9.1.2 Toegang tot netwerken en netwerkdiensten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Y	Een beleid voor het gebruik van netwerken en netwerkdiensten behoort te worden geformuleerd. Dit beleid behoort te omvatten: a) de netwerken en netwerkdiensten waartoe toegang wordt verleend; b) autorisatieprocedures om vast te stellen wie toegang krijgt tot welk netwerk en welke netwerkdiensten; c) beheersmaatregelen en -procedures om de toegang tot netwerkverbindingen en -diensten te beschermen;	

		d) de middelen die worden gebruikt om toegang te krijgen tot netwerken en netwerkdiensten (bijv. VPN of draadloos netwerk); e) eisen voor gebruikersauthenticatie voor de toegang tot de verschillende netwerkdiensten; f) monitoren van het gebruik van netwerkdiensten. Het beleid voor het gebruik van netwerkdiensten behoort aan te sluiten bij het toegangsbeveiligingsbeleid van de organisatie (zie 9.1.1).	

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 afmelden van gebruikers

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Y	De procedure voor het beheren van gebruikersidentificaties behoort te omvatten: a) het gebruik van unieke gebruikersidentificaties zodat gebruikers kunnen worden gekoppeld aan en verantwoordelijk kunnen worden gesteld voor hun acties; het gebruik van groepsidentificaties behoort alleen te worden toegelaten als deze om bedrijfs- of operationele redenen noodzakelijk zijn en behoort te worden goedgekeurd en gedocumenteerd; b) het onmiddellijk ongeldig maken of verwijderen van de gebruikersidentificatie van gebruikers die de organisatie hebben verlaten (zie 9.2.6); c) het periodiek identificeren en verwijderen van overbodige gebruikersidentificaties; d) het ervoor zorgen dat overtollige gebruikersidentificaties niet aan andere gebruikers worden uitgegeven.	Het is belangrijk te begrijpen dat de taak van het identificeren en registreren van gebruikers van gezondheidsinformatiesystemen ook alle volgende punten omvat: a) het nauwkeurig vastleggen van de identiteit van een gebruiker (bijv. Jan Smit, geboren op 26 maart 1982, momenteel woonachtig op een specifiek adres); b) het nauwkeurig vastleggen, na verificatie, van de blijvende beroepsgegevens van een gebruiker (bijv. Dr. Suzan Jansen, cardioloog) en/of functiebenaming (bijv. Jan Smit , medisch receptionist); c) het toewijzen van een ondubbelzinnige gebruikersidentificatiecode. Let op: patiënten zijn meestal geen systeemgebruikers, hoewel de patiënten die online toegang hebben tot (een deel van) hun persoonlijke gegevens (bijv. via een online portal) wel systeemgebruikers kunnen zijn (zij het dat ze beperkte toegang hebben). Ook zijn er gezondheidstoepassingen waarin een gebruiker algemene gezondheidsadviezen en -informatie kan zoeken. Hoewel dit verzoek tot informatie geregistreerd kan worden, blijft de gebruiker die toegang maakt tot dit systeem, anoniem. Veel websites die informatie geven over zwangerschap, aids of andere volksgezondheidsonderwerpen, werken zo. Gebruikers van dergelijke algemene informatiesites hoeven zich meestal niet te registreren en worden daarom niet in aanmerking genomen in de bespreking die hieronder volgt. Zie ook 7.2.1.

A.9.2.2 Gebruikers toegang verlenen			
Beheersmaatregel (ISO 27001)	**SOA**	**Implementatierichtlijn**	**Zorgspecifieke implementatierichtlijn**
Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	Y	De procedure voor het toewijzen of intrekken van toegangsrechten aan gebruikersidentificaties behoort te omvatten: a) autorisatie verkrijgen van de eigenaar van het informatiesysteem of de informatiedienst voor het gebruik van het informatiesysteem of de informatiedienst (zie beheersmaatregel 8.1.2); afzonderlijke goedkeuring voor toegangsrechten door de directie is mogelijk ook relevant; b) verifiëren dat het verleende toegangsniveau in overeenstemming is met de beleidsregels voor toegang (zie 9.1) en consistent is met andere eisen zoals een scheiding van taken (zie 6.1.2); c) waarborgen dat toegangsrechten niet worden geactiveerd (bijv. door dienstverleners) voordat de autorisatieprocedures zijn afgerond; d) bijhouden van een centraal overzicht van toegangsrechten die aan een gebruikersidentificatie zijn toegekend om toegang te verkrijgen tot informatiesystemen en -diensten; e) aanpassen van toegangsrechten van gebruikers van wie de rollen of functies zijn gewijzigd en toegangsrechten van gebruikers die de organisatie hebben verlaten onmiddellijk verwijderen of blokkeren; f) met eigenaren van de informatiesystemen of -diensten periodiek de toegangsrechten beoordelen (zie 9.2.5).	In procedures voor het verlenen van toegang aan gebruikers behoort duidelijk te worden vastgesteld of gebruikers al dan niet toegang krijgen tot persoonlijke gezondheidsinformatie.
A.9.2.3 Beheren van speciale toegangsrechten			
Beheersmaatregel (ISO 27001)	**SOA**	**Implementatierichtlijn**	**Zorgspecifieke implementatierichtlijn**
Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Y	Het toewijzen van speciale toegangsrechten behoort te worden beheerst door een formele autorisatieprocedure die in overeenstemming is met het relevante toegangsbeveiligingsbeleid (zie beheersmaatregel 9.1.1). De volgende stappen behoren in overweging te worden genomen: a) de speciale toegangsrechten behorend bij elk systeem of proces, bijv. besturingssysteem, databasebeheersysteem en elke toepassing, en de gebruikers aan wie ze moeten worden toegewezen, behoren te worden geïdentificeerd; b) speciale toegangsrechten behoren op basis van noodzaak tot gebruik en per gebeurtenis aan gebruikers te worden toegekend in overeenstemming met het toegangsbeveiligingsbeleid (zie 9.1.1), d.w.z. gebaseerd op wat minimaal is vereist voor hun functionele rollen; c) er behoort een autorisatieprocedure en een verslaglegging van alle toegekende speciale toegangsrechten te worden bijgehouden. Speciale toegangsrechten behoren niet te worden verleend voordat de autorisatieprocedure is afgerond; d) voor het vervallen van speciale toegangsrechten behoren eisen te worden gedefinieerd; e) speciale toegangsrechten behoren te worden toegekend aan een gebruikersidentificatie die verschilt van identiteiten die voor reguliere bedrijfsactiviteiten worden gebruikt. Reguliere bedrijfsactiviteiten behoren niet met een speciale gebruikersidentificatie te worden verricht;	In de bespreking die hieronder volgt, wordt een aantal strategieën gespecificeerd voor toegangsbeheersmaatregelen die aanmerkelijk kunnen helpen bij het garanderen van de vertrouwelijkheid en integriteit van persoonlijke gezondheidsinformatie. Deze zijn: a) op rollen gebaseerde toegangscontrole die gebruikmaakt van de beroepsgegevens en/of functiebenamingen van gebruikers die tijdens het registreren zijn vastgesteld om de toegangsrechten van gebruikers te beperken tot de rechten die vereist zijn om een of meer goed gedefinieerde rollen te vervullen; b) op werkgroepen gebaseerde toegangscontrole die werkt met de toewijzing van gebruikers aan werkgroepen (zoals klinische teams) om te bepalen tot welke registraties zij toegang hebben; c) discretionaire toegangscontrole die gebruikers van gezondheidsinformatiesystemen die een legitieme relatie hebben met de persoonlijke

		f) de competenties van gebruikers met speciale toegangsrechten behoren regelmatig te worden beoordeeld om te verifiëren of ze in overeenstemming zijn met hun taken; g) specifieke procedures behoren te worden vastgesteld en onderhouden om onbevoegd gebruik van gebruikersidentificaties voor algemeen beheer te voorkomen, in overeenstemming met de configuratiecapaciteiten van het systeem. h) voor gebruikersidentificaties voor algemeen beheer behoort de geheimhouding van geheime authenticatie-informatie in acht te worden genomen als deze wordt gedeeld (bijv. vaak veranderen van wachtwoord en zodra een speciale gebruiker vertrekt of van functie verandert, dit onder speciale gebruikers communiceren met de passende mechanismen).	gezondheidsinformatie van de patiënt (bijv. een huisarts), in staat stelt toegang te verlenen aan andere gebruikers die geen eerder tot stand gebrachte relatie met de persoonlijke gezondheidsinformatie van die patiënt hebben (bijv. een specialist). Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie bevatten, behoren op rollen gebaseerde toegangscontrole te ondersteunen waarmee elke gebruiker aan een of meer rollen kan worden toegewezen en elke rol aan een of meer systeemfuncties. Een gebruiker van een gezondheidsinformatiesysteem dat persoonlijke gezondheidsinformatie bevat, behoort in één rol toegang te hebben met de diensten ervan (d.w.z. dat gebruikers die met meer dan één rol geregistreerd zijn, tijdens elke sessie waarin ze toegang hebben tot het gezondheidsinformatiesysteem één rol behoren aan te geven). Gezondheidsinformatiesystemen behoren gebruikers (waaronder begrepen zorgverleners, ondersteunend personeel en anderen) aan de registraties van patiënten te koppelen en toekomstige toegang op basis van deze koppeling mogelijk te maken. Aanvullende richtlijnen over rechtenmanagement in de zorg zijn te vinden in ISO 22600-1 en in ISO 22600-2.

A.9.2.4 Beheer van geheime authenticatie-informatie van gebruikers

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Y	Het proces behoort de volgende eisen te bevatten: a) gebruikers behoren te worden verplicht een verklaring te ondertekenen dat zij persoonlijke geheime authenticatie-informatie geheimhouden en groepsinformatie, d.w.z. gedeelde geheime authenticatie-informatie, binnen de groep houden; deze getekende verklaring kan worden opgenomen in de arbeidsvoorwaarden (zie 7.1.2); b) als gebruikers hun eigen geheime authenticatie-informatie moeten onderhouden, behoort hun eerst tijdelijke geheime authenticatie-informatie te worden gegeven die zij bij het eerste gebruik moeten wijzigen; c) er behoren procedures te worden vastgesteld om de identiteit van een gebruiker vast te stellen voordat nieuwe, vervangende of tijdelijke geheime authenticatie-informatie wordt verstrekt; d) tijdelijke geheime authenticatie-informatie behoort op een veilige manier aan gebruikers te worden gegeven; gebruikmaken van externe partijen of onbeschermde e-mailberichten (niet-gecodeerde tekst) behoort te worden vermeden; e) tijdelijke geheime authenticatie-informatie behoort uniek voor een persoon te zijn en behoort niet te kunnen worden geraden; f) gebruikers behoren de ontvangst van geheime authenticatie-informatie te bevestigen;	Er is geen aanvullende richtlijn voor informatiebeveiligingsbeheer binnen de zorg, hoewel hier behoort te worden opgemerkt dat de tijdsdruk binnen zorgverleningssituaties doeltreffend gebruik van wachtwoorden lastig kan maken. Veel gezondheidsorganisaties hebben het invoeren van alternatieve authenticatietechnologieën met het oog op dit probleem in overweging genomen.

		g) 'default' geheime authenticatie-informatie van een leverancier behoort te worden gewijzigd na de installatie van systemen of software.	

A.9.2.5 Beoordeling van toegangsrechten van gebruikers

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Y	Bij het beoordelen van toegangsrechten van gebruikers behoren de volgende aspecten in overweging te worden genomen: a) toegangsrechten van gebruikers behoren regelmatig en na wijzigingen, zoals promotie, degradatie of beëindiging van het dienstverband, te worden beoordeeld (zie hoofdstuk 7); b) toegangsrechten van gebruikers behoren te worden beoordeeld en opnieuw te worden toegekend bij functieverandering binnen dezelfde organisatie; c) autorisaties voor speciale toegangsrechten behoren vaker te worden beoordeeld; d) toewijzingen van speciale toegangsrechten behoren regelmatig te worden gecontroleerd om te waarborgen dat speciale toegangsrechten niet onbevoegd zijn verkregen; e) van wijzigingen in speciale accounts behoren voor periodieke beoordeling logbestanden te worden bijgehouden.	Er behoort speciaal rekening te worden gehouden met gebruikers van wie in redelijkheid zal worden verwacht dat ze noodzorg verlenen waarbij het nodig kan zijn dat zij toegang tot persoonlijke gezondheidsinformatie hebben in een noodsituatie waarin een patiënt wellicht niet in staat is aan te geven daarmee in te stemmen.

A.9.2.6 Toegangsrechten intrekken of aanpassen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	Y	Bij beëindiging van het dienstverband behoren de toegangsrechten van een persoon voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten en diensten te worden ingetrokken of opgeschort. Hierdoor kan worden vastgesteld of het noodzakelijk is om toegangsrechten in te trekken. Wijzigingen in het dienstverband behoren te worden weerspiegeld in het intrekken van alle toegangsrechten die niet voor het nieuwe dienstverband zijn goedgekeurd. De toegangsrechten die behoren te worden ingetrokken of aangepast omvatten ook de fysieke en logische toegangsrechten. Intrekking of aanpassing kan plaatsvinden door verwijdering, intrekking of vervanging van sleutels, identificatiekaarten, informatieverwerkende faciliteiten of abonnementen. Elk document dat toegangsrechten van medewerkers en contractanten identificeert, behoort de intrekking of aanpassing van toegangsrechten weer te geven. Indien een medewerker die uit dienst gaat of een externe gebruiker wachtwoorden kent van gebruikersidentificaties die actief blijven, dan behoren deze bij beëindiging of wijziging van dienstverband, contract of overeenkomst te worden gewijzigd. Toegangsrechten voor informatie en bedrijfsmiddelen die samenhangen met informatieverwerkende faciliteiten behoren te worden verminderd of ingetrokken voordat het dienstverband eindigt of wijzigt, afhankelijk van de evaluatie van risicofactoren zoals: a) of de beëindiging of wijziging is geïnitieerd door de medewerker, de externe gebruiker of door de directie, en de reden voor de beëindiging; b) de huidige verantwoordelijkheden van de medewerker, externe gebruiker of overige gebruikers; c) de waarde van de bedrijfsmiddelen die op dat moment toegankelijk zijn.	Het is belangrijk om te wijzen op de vele voorbeelden in de zorg van studenten, stagiairs en vervangers die hun toegangsrechten hebben behouden na beëindiging van hun stage, vervanging enz. Met name in grote ziekenhuizen hebben vaak grote aantallen tijdelijk personeel kortstondig toegang tot persoonlijke gezondheidsinformatie. Het beëindigen van de toegangsrechten van dergelijk personeel behoort zorgvuldig te worden gemanaged. Tegelijkertijd vinden in de zorg veel transacties geruime tijd na het moment van zorgverlening plaats (bijv. het aftekenen van medische transcripties). Dit kan het proces van het tijdig verwijderen van toegangsrechten aanmerkelijk gecompliceerder maken en met deze transacties behoort rekening te worden gehouden bij het ontwerpen en implementeren van procedures voor het verwijderen van toegangsrechten. Gezondheidsorganisaties behoren serieus na te denken over het onmiddellijk beëindigen van toegangsrechten na ontvangst of verzending van een ontslagbrief of een kennisgeving van ontslag enz., als men dan van mening is dat het voortzetten van die toegang een verhoogd risico met zich meebrengt.

A.9.3 Verantwoordelijkheden van gebruikers

Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatieinformatie

A.9.3.1 Geheime authenticatieinformatie gebruiken

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatieinformatie houden aan de praktijk van de organisatie.	Y	Alle gebruikers behoren het advies te krijgen om: a) vertrouwelijk om te gaan met geheime authenticatie-informatie, en ervoor te zorgen dat deze informatie niet openbaar wordt gemaakt aan andere partijen, met inbegrip van gezaghebbende personen; b) geen geheime authenticatie-informatie te registreren (bijv. op papier, in een computerbestand of op een zakapparaat), tenzij deze informatie veilig kan worden opgeslagen en de opslagmethode is goedgekeurd (bijv. 'password vault'); c) geheime authenticatie-informatie te wijzigen als er een aanwijzing is dat deze mogelijk is gecompromitteerd; d) als wachtwoorden als geheime authenticatie-informatie worden gebruikt, sterke wachtwoorden te kiezen van voldoende minimumlengte, die: 1) gemakkelijk te onthouden zijn; 2) niet zijn gebaseerd op gegevens die iemand anders gemakkelijk kan raden of achterhalen door persoonsgerelateerde informatie te gebruiken, zoals namen, telefoonnummers en geboortedata; 3) niet kwetsbaar zijn voor woordenboekaanvallen (d.w.z. niet bestaan uit woorden die in woordenboeken zijn opgenomen); 4) geen opeenvolgende identieke tekens bevat, en niet alleen uit cijfers of letters bestaat; 5) bij het eerste inloggen worden gewijzigd als ze tijdelijk zijn; e) geen geheime authenticatie-informatie te delen; f) te zorgen voor passende bescherming van wachtwoorden wanneer wachtwoorden worden gebruikt als geheime authenticatie-informatie in geautomatiseerde inlogprocedures en worden opgeslagen; g) niet dezelfde geheime authenticatie-informatie voor zakelijke en particuliere toepassingen te gebruiken.	Organisaties die gezondheidsinformatie verwerken, behoren bij het bepalen van de verantwoordelijkheden van gebruikers de rechten en ethische verantwoordelijkheden van zorgverleners, zoals wettelijk overeengekomen en aanvaard door leden van organisaties van zorgverleners, te respecteren.

A.9.4 Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen

A.9.4.1 Beperking toegang tot informatie

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Y	Toegangsbeperkingen behoren te worden gebaseerd op eisen voor de afzonderlijke bedrijfstoepassingen en in overeenstemming met het beleid dat voor toegangsbeveiliging is gedefinieerd. De volgende aspecten behoren in aanmerking te worden genomen om de eisen voor toegangsbeperking te ondersteunen: a) menu's verschaffen om de toegang tot systeemfuncties van toepassingen te beheersen; b) beheersen welke gegevens voor een bepaalde gebruiker toegankelijk zijn;	Er behoort speciale aandacht te worden besteed aan de technische maatregelen waardoor de identiteit van een patiënt op beveiligde wijze wordt vastgesteld als hij of zij toegang maakt tot (een deel van) zijn/haar eigen informatie (in die gezondheidsinformatiesystemen die zulke toegang toestaan). Er behoort ook een soortgelijke nadruk te worden gelegd op het gebruiksgemak van

		c) toegangsrechten van gebruikers beheersen, bijv. lezen, schrijven, verwijderen en uitvoeren; d) toegangsrechten voor andere toepassingen beheersen; e) de informatie in output beperken; f) zorgen voor fysieke of logische toegangsbeveiligingsmaatregelen voor het isoleren van gevoelige toepassingen, toepassingsgegevens of systemen.	dergelijke maatregelen, met name voor gehandicapte patiënten en op voorzieningen voor toegang door vervangende besluitvormers.

A.9.4.2 Beveiligde inlogprocedures

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Y	Om de geclaimde identiteit van een gebruiker te bewijzen behoort een passende authenticatietechniek te worden gekozen. Ingeval krachtige verificatie en authenticatie van de identiteit is vereist behoren andere authenticatiemethoden dan wachtwoorden te worden gebruikt, zoals cryptografische middelen, chipkaarten, tokens of biometrische middelen. De procedure om in een systeem in te loggen behoort zo te worden ontworpen dat de kans op onbevoegde toegang zo klein mogelijk wordt gemaakt. Om te voorkomen dat het een onbevoegde gebruiker gemakkelijk wordt gemaakt behoort de inlogprocedure zo min mogelijk informatie over het systeem of de toepassing openbaar te maken. Een goede inlogprocedure behoort: a) geen systeem- of toepassingsidentificatoren te tonen voordat het inlogproces met succes is afgerond; b) een algemene waarschuwing te tonen dat de computer alleen toegankelijk is voor bevoegde gebruikers; c) tijdens de inlogprocedure geen hulpboodschappen weer te geven waarmee onbevoegde gebruikers hun doel kunnen bereiken; d) de inloginformatie pas na invoer van alle gegevens te valideren. Indien zich een fout voordoet, behoort het systeem niet aan te geven welk deel van de gegevens juist of onjuist is; e) bescherming te bieden tegen inlogpogingen die met grove middelen worden uitgevoerd; f) niet-succesvolle en succesvolle pogingen te registreren; g) een informatiebeveiligingsgebeurtenis te initiëren als een poging tot of een succesvolle schending van de inlogbeheersmaatregelen is vastgesteld; h) de volgende informatie te tonen nadat het inloggen met succes is voltooid: 1) datum en tijdstip waarop de vorige keer met succes is ingelogd; 2) details van niet-succesvolle pogingen om in te loggen sinds de vorige succesvolle poging om in te loggen; i) een wachtwoord dat wordt ingevoerd niet weer te geven; j) geen ongecodeerde wachtwoorden via een netwerk te versturen; k) inactieve sessies na een bepaalde tijd van inactiviteit te beëindigen, vooral op locaties met een hoog risico, zoals openbare of externe locaties die buiten het beveiligingsbeheer van de organisatie vallen, of op mobiele apparaten; l) de verbindingstijd te beperken om extra beveiliging te bieden voor toepassingen met een hoog risico en de mogelijkheden voor onbevoegde toegang te verkleinen.	

A.9.4.3 Systeem voor wachtwoordbeheer

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn

Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Y	Een systeem voor wachtwoordbeheer behoort: a) het gebruik van individuele gebruikersidentificaties en wachtwoorden af te dwingen om de toerekenbaarheid te handhaven; b) gebruikers de mogelijkheid te bieden hun eigen wachtwoord te kiezen en te wijzigen, en een bevestigingsprocedure te bevatten die rekening houdt met foutieve invoer; c) de keuze voor sterke wachtwoorden af te dwingen; d) gebruikers te dwingen hun wachtwoord bij het eerste inloggen te wijzigen; e) wijziging van het wachtwoord periodiek en telkens wanneer dat nodig is af te dwingen; f) een registratie van eerder gebruikte wachtwoorden bij te houden en te voorkomen dat deze opnieuw worden gebruikt; g) wachtwoorden niet op het scherm te tonen als ze worden ingevoerd; h) wachtwoordbestanden apart van systeemgegevens van toepassingen op te slaan; i) wachtwoorden in beschermde vorm op te slaan en te versturen.	

A.9.4.4 Speciale systeemhulpmiddelen gebruiken

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	***N***	Voor het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoren de volgende richtlijnen te worden overwogen: a) gebruik van identificatie-, authenticatie- en autorisatieprocedures voor systeemhulpmiddelen; b) scheiding van systeemhulpmiddelen en toepassingssoftware; c) beperking van het gebruik van systeemhulpmiddelen tot het laagste aantal betrouwbare bevoegde gebruikers dat praktisch haalbaar is (zie 9.2.3); d) autorisatie voor ad-hocgebruik van systeemhulpmiddelen; e) beperking van de beschikbaarheid van systeemhulpmiddelen, bijv. voor de duur van een geautoriseerde wijziging; f) registreren van alle gebruik van systeemhulpmiddelen; g) definiëren en documenteren van autorisatieniveaus voor systeemhulpmiddelen; h) verwijderen of onbruikbaar maken van alle onnodige systeemhulpmiddelen; i) niet beschikbaar stellen van systeemhulpmiddelen aan gebruikers die toegang hebben tot toepassingen op systemen waarbij scheiding van taken vereist is.	

A.9.4.5 Toegangsbeveiliging op programmabroncode

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Toegang tot de programmabroncode behoort te worden beperkt.	***N***	Toegang tot programmabroncodes en samenhangende items (zoals ontwerpen, specificaties, verificatie- en validatieschema's) behoort strikt te worden beheerst om de introductie van onbevoegde functionaliteit en om onbedoelde wijzigingen te voorkomen, alsmede om de vertrouwelijkheid van waardevolle intellectuele eigendom te handhaven. Met betrekking tot de programmabroncode kan dit worden bereikt door de code gecontroleerd centraal op te slaan, bij voorkeur in de broncodebibliotheek. De volgende richtlijnen behoren dan te worden overwogen om de toegang tot dergelijke broncodebibliotheken te beheersen en zo de kans op corruptie van computerprogramma's te verkleinen. a) waar mogelijk, behoren broncodebibliotheken niet in operationele systemen te worden opgeslagen; b) de programmabroncode en de broncodebibliotheek behoren te worden beheerd in overeenstemming met vastgestelde procedures;	

		c) ondersteunend personeel behoort geen onbeperkte toegang tot broncodebibliotheken te hebben; d) het updaten van broncodebibliotheken en samenhangende items en het verstrekken van broncodes aan programmeurs behoort alleen plaats te vinden na ontvangst van een passende autorisatie; e) programma-uitdraaien behoren in een beveiligde omgeving te worden bewaard; f) van elke toegang tot broncodebibliotheken behoort een auditlogbestand te worden bijgehouden; g) onderhouden en kopiëren van broncodebibliotheken behoren aan strikte procedures voor wijzigingsbeheer te worden onderworpen (zie 14.2.2). Indien het de bedoeling is dat de programmabroncode wordt gepubliceerd behoren aanvullende beheersmaatregelen die bijdragen aan het waarborgen van de integriteit ervan (bijv. een digitale handtekening) te worden overwogen.	

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	***N***	Bij het ontwikkelen van een cryptografiebeleid behoren de volgende aspecten in aanmerking te worden genomen: a) de manier waarop de directie het gebruik van cryptografische beheersmaatregelen in de gehele organisatie benadert, met inbegrip van de algemene principes die gelden voor de bescherming van de bedrijfsinformatie; b) het vereiste beschermingsniveau behoort te worden geïdentificeerd op basis van een risicobeoordeling, rekening houdend met type, sterkte en kwaliteit van het vereiste versleutelingsalgoritme; c) het gebruik van versleuteling ter bescherming van informatie die wordt vervoerd per draagbare of verwijderbare media-apparatuur of via communicatiekanalen; d) de aanpak van sleutelbeheer, waaronder methoden ter bescherming van cryptografische sleutels en het herstel van versleutelde informatie in geval van verloren, gecompromitteerde of beschadigde sleutels; e) rollen en verantwoordelijkheden, bijv. wie is verantwoordelijk voor: 1) het implementeren van het beleid; 2) het sleutelbeheer, waaronder het aanmaken van sleutels (zie 10.1.2); f) de normen die moeten worden toegepast voor een doeltreffende implementatie in de gehele organisatie (welke oplossing wordt gebruikt voor welk bedrijfsproces); g) de impact van het gebruik van versleutelde informatie op beheersmaatregelen die zijn gebaseerd op controle van de inhoud (bijv. detectie van malware).	Richtlijnen over beleid voor het uitgeven en gebruiken van digitale certificaten in de zorg en over het sleutelbeheer zijn te vinden in ISO 17090-3.

		Bij het implementeren van het cryptografiebeleid behoort rekening te worden gehouden met de regelgeving en nationale beperkingen die kunnen gelden voor het gebruik van cryptografische technieken in verschillende delen van de wereld en met problemen met grensoverschrijdende stromen van versleutelde informatie (zie 18.1.5). Cryptografische beheersmaatregelen kunnen worden gebruikt voor verschillende informatiebeveiligingsdoelstellingen, bijv.: a) vertrouwelijkheid: codering van informatie gebruiken om gevoelige of essentiële informatie, tijdens opslag of verzending, te beschermen; b) integriteit/authenticiteit: digitale handtekeningen of authenticatiecodes voor berichten gebruiken om de authenticiteit of integriteit van gevoelige of essentiële informatie tijdens opslag of verzending te verifiëren; c) onweerlegbaarheid: cryptografische technieken gebruiken om bewijs te verkrijgen van het al dan niet plaatsvinden van een gebeurtenis of actie; d) authenticatie: cryptografische technieken gebruiken ter authenticatie van gebruikers en andere systeementiteiten die toegang vragen tot of die verrichtingen doen met systeemgebruikers, entiteiten en -bronnen.	

A.10.1.2 Sleutelbeheer

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	***Y***	Het beleid behoort eisen te bevatten voor het beheren van cryptografische sleutels tijdens hun gehele levenscyclus met inbegrip van het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van sleutels. Cryptografische algoritmen, sleutellengte en gebruikspraktijken behoren te worden geselecteerd in overeenstemming met de 'best practices'. Passend sleutelbeheer vereist nauwkeurige procedures voor het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van cryptografische sleutels. Alle cryptografische sleutels behoren te worden beschermd tegen aanpassing en verlies. Bovendien hebben geheime en particuliere sleutels bescherming nodig tegen onbevoegd gebruik en tegen openbaarmaking. Apparatuur die wordt gebruikt om sleutels aan te maken, op te slaan en te archiveren behoort fysiek te worden beschermd. Een sleutelbeheersysteem behoort te zijn gebaseerd op een overeengekomen pakket van normen, procedures en beveiligingsmethoden voor: a) het aanmaken van sleutels voor verschillende cryptografische systemen en verschillende toepassingen; b) het verstrekken en verkrijgen van openbare sleutelcertificaten; c) het verspreiden van sleutels onder de beoogde entiteiten en een instructie hoe de sleutels na ontvangst behoren te worden geactiveerd; d) het opslaan van sleutels en de wijze waarop bevoegde gebruikers toegang tot sleutels krijgen; e) het wijzigen of updaten van sleutels, met inbegrip van regels over wanneer en hoe sleutels behoren te worden gewijzigd; f) het omgaan met gecompromitteerde sleutels; g) het intrekken van sleutels, met inbegrip van hoe sleutels behoren te worden teruggetrokken of gedeactiveerd, bijv. als sleutels zijn gecompromitteerd of als een gebruiker de organisatie verlaat (in welk geval sleutels ook behoren te worden gearchiveerd);	Richtlijnen over sleutelbeheer zijn te vinden in ISO 17090-3. Bij deze richtlijnen dient men zich te beperken tot het beheer van de certificaten aan de klantzijde.

		h) het herstellen van sleutels die verloren of gecorrumpeerd zijn; i) het back-uppen of archiveren van sleutels; j) het vernietigen van sleutels; k) het registreren en auditen van aan sleutelbeheer gerelateerde activiteiten. Om de kans op onjuist gebruik te verkleinen behoren de activerings- en deactiveringsdatum van sleutels te worden vastgesteld zodat de sleutels alleen kunnen worden gebruikt tijdens de periode die in het desbetreffende sleutelbeheerbeleid is vastgesteld. Naast het zorgvuldig beheren van geheime en persoonlijke sleutels behoort ook aandacht te worden besteed aan de authenticiteit van openbare sleutels. Deze authenticatieprocedure kan worden uitgevoerd met gebruikmaking van openbaresleutelcertificaten, die gewoonlijk worden uitgegeven door een certificerende instantie, die een erkende organisatie behoort te zijn die beschikt over passende beheersmaatregelen en procedures om de vereiste mate van betrouwbaarheid te kunnen leveren. De inhoud van dienstverleningsovereenkomsten of contracten met externe leveranciers van cryptografische diensten, bijv. met een certificerende instantie, behoort aansprakelijkheid, betrouwbaarheid van dienstverlening en responstijden voor dienstverlening te omvatten (zie 15.2)	

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Y	Voor zover van toepassing behoren de volgende richtlijnen voor fysieke beveiligingszones te worden overwogen: a) beveiligingszones behoren te worden gedefinieerd, en de locatie en sterkte van elke zone behoren af te hangen van de beveiligingseisen van de bedrijfsmiddelen die zich binnen de zone bevinden en van de resultaten van een risicobeoordeling; b) de begrenzing van een gebouw of locatie waarin zich informatieverwerkende faciliteiten bevinden, behoort fysiek in orde te zijn (d.w.z. er behoren geen openingen in de begrenzing te zijn en er behoren geen ruimten te zijn waar gemakkelijk kan worden ingebroken); het dak, de muren en vloer van de locatie behoren solide te zijn en alle buitendeuren behoren passend tegen onbevoegde toegang te zijn beschermd met controlemechanismen (bijv. afsluitbomen, alarmsystemen, sloten); deuren en ramen behoren afgesloten te zijn als er niemand aanwezig is, en voor ramen, in het bijzonder die op de begane grond, behoort externe bescherming te worden overwogen; c) er behoort een bemande receptie of andere voorziening ter controle van de fysieke toegang tot de locatie of het gebouw aanwezig te zijn; toegang tot locaties en gebouwen behoort te worden beperkt tot bevoegd personeel; d) er behoren, indien van toepassing, fysieke hindernissen te worden aangebracht om onbevoegde fysieke toegang en vervuiling van de omgeving te voorkomen; e) alle branddeuren in een beveiligde zone behoren te worden voorzien van alarm, te worden gemonitord en getest in combinatie met de muren om het vereiste niveau van	Het is belangrijk te erkennen dat in veel zorgsituaties het inrichten van beveiligde zones zeer uitdagend is. In veel operationele gebieden zijn patiënten aanwezig. Er is wellicht geen andere bedrijfstak waar het publiek zo veel toegang tot operationele gebieden heeft als in de zorg. Tegelijkertijd behoort er een veilige omgeving te worden gehandhaafd die de fysieke veiligheid en beveiliging van patiënten en van de gegevens en systemen die binnen die omgeving toegankelijk kunnen zijn, in stand houdt. Het is bijvoorbeeld mogelijk dat een patiënt alleen wordt achtergelaten in een onderzoekskamer (bijv. om de patiënt een onderzoeksschort te laten aantrekken voor een lichamelijk onderzoek), ondanks dat er een werkend werkstation in het vertrek aanwezig is. De beveiliging van werkstations in de zorg mag daarom niet volledig afhangen van het uit beveiligde zones buitensluiten van patiënten. Dit in tegenstelling tot een bank bijvoorbeeld, waar klanten waarschijnlijk nooit alleen zouden worden gelaten in een omgeving met een werkend werkstation.

		brandwerendheid in overeenstemming met passende regionale, nationale en internationale normen vast te stellen; de werking van de deuren behoort, in overeenstemming met de plaatselijke brandcode, faalveilig te zijn; f) tegen indringers behoren op alle buitendeuren en toegankelijke ramen passende detectiesystemen in overeenstemming met nationale, regionale of internationale normen te worden geïnstalleerd en regelmatig getest; onbemande ruimten behoren te allen tijde te zijn voorzien van een alarmsysteem; ook andere ruimten, bijv. de computer- of communicatieruimten, behoren te worden bestreken door het alarmsysteem; informatieverwerkende faciliteiten die worden beheerd door de organisatie behoren fysiek te zijn gescheiden van informatieverwerkende faciliteiten die door externe partijen worden beheerd.	Bovendien zijn patiënten in de zorg in tegenstelling tot patiënten in andere bedrijfstakken vaak fysiek niet in staat te voorzien in hun eigen persoonlijke veiligheid en beveiliging. Fysieke beveiligingsmaatregelen voor informatie behoren te worden afgestemd op fysieke beveiligings- en veiligheidsmaatregelen voor patiënten. Zorginstellingen hebben een plicht om deze beide te beschermen.

A.11.1.2 Fysieke toegangsbeveiliging

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Y	Met de volgende richtlijnen behoort rekening te worden gehouden: a) datum en tijdstip van binnenkomst en vertrek van bezoekers behoort te worden geregistreerd, en op alle bezoekers behoort toezicht te worden gehouden tenzij hun toegang vooraf is goedgekeurd; personen behoort alleen toegang te worden verleend voor specifieke, goedgekeurde doelen, en zij behoren instructies over de beveiligingseisen van het gebied en de noodprocedures te ontvangen. De identiteit van bezoekers behoort met passende middelen te worden vastgesteld; b) toegang tot gebieden waar vertrouwelijke informatie wordt verwerkt of opgeslagen behoort te worden beperkt tot bevoegde personen door passende toegangsbeveiligingsmaatregelen te implementeren, bijv. door het implementeren van een dubbel authenticatiemechanisme zoals een toegangskaart en een geheime pincode; c) van elke toegang behoort een fysiek logboek of een elektronisch audittraject te worden onderhouden en gemonitord; d) van alle medewerkers, contractanten en externe partijen behoort te worden verlangd dat zij een bepaalde vorm van zichtbare identificatie dragen en zij behoren onmiddellijk beveiligingspersoneel te informeren als zij bezoekers zonder begeleiding en personen die geen zichtbare identificatie dragen, tegenkomen; e) personeel van externe partijen die ondersteunende diensten verlenen, behoort alleen indien noodzakelijk beperkte toegang tot beveiligde gebieden of faciliteiten die vertrouwelijke informatie verwerken te worden verleend; deze toegang behoort te worden goedgekeurd en gemonitord; f) toegangsrechten voor beveiligde gebieden behoren regelmatig te worden beoordeeld, geactualiseerd en indien nodig te worden ingetrokken (zie 9.2.5 en 9.2.6).	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren zinnige maatregelen te treffen om te garanderen dat het publiek slechts zo dicht bij IT-uitrusting (servers, opslagapparaten, terminals en displays) kan komen als de fysieke beperkingen en klinische processen vereisen.

A.11.1.3 Kantoren, ruimten en faciliteiten beveiligen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Y	Bij het beveiligen van kantoren, ruimten en faciliteiten behoren de volgende richtlijnen in aanmerking te worden genomen: a) belangrijke faciliteiten behoren zo te worden gesitueerd dat ze niet voor iedereen toegankelijk zijn;	

		b) indien van toepassing behoren gebouwen onopvallend te zijn en zo min mogelijk aanwijzingen te geven over het gebruiksdoel ervan, zonder duidelijke tekenen, binnen of buiten het gebouw, die op de aanwezigheid van informatieverwerkende activiteiten duiden; c) faciliteiten behoren zo te zijn geconfigureerd dat wordt voorkomen dat vertrouwelijke informatie of activiteiten van buitenaf zichtbaar en hoorbaar zijn. Voor zover van toepassing behoort elektromagnetische afscherming ook te worden overwogen; d) adresboeken en interne telefoonboeken waarin locaties worden aangeduid met faciliteiten die vertrouwelijke informatie verwerken, behoren niet vrij toegankelijk te zijn voor onbevoegden.	

A.11.1.4 Beschermen tegen bedreigingen van buitenaf

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Y	Over het vermijden van schade door brand, overstroming, aardbeving, explosie, oproer en andere vormen van natuurrampen of door personen veroorzaakte rampen behoort specialistisch advies te worden ingewonnen.	

A.11.1.5 Werken in beveiligde gebieden

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	***N***	Met de volgende richtlijnen behoort rekening te worden gehouden: a) personeel behoort alleen op grond van 'need-to-know' bekend te zijn met het bestaan van of de activiteiten in een beveiligd gebied. b) zonder toezicht werken in beveiligde gebieden behoort te worden vermeden, zowel om veiligheidsredenen als om geen gelegenheid te bieden voor kwaadaardige activiteiten; c) leegstaande beveiligde ruimten behoren fysiek te worden afgesloten en periodiek te worden geïnspecteerd; d) foto-, video-, audio- of andere opnameapparatuur, zoals camera's in mobiele apparatuur, behoort, tenzij goedgekeurd, niet te worden toegelaten. De afspraken voor het werken in beveiligde zones bevatten beheersmaatregelen voor de medewerkers en voor externe gebruikers die in de beveiligde zone werken en beslaan alle activiteiten die in de beveiligde zone plaatsvinden.	

A.11.1.6 Laad- en loslocatie

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Y	Met de volgende richtlijnen behoort rekening te worden gehouden: a) toegang tot een laad- en loslocatie van buiten het gebouw behoort te worden beperkt tot geïdentificeerd en bevoegd personeel; b) de laad- en loslocatie behoort zo te zijn ontworpen dat goederen kunnen worden geladen en gelost zonder dat de leverancier toegang heeft tot andere delen van het gebouw; c) de buitendeuren van een laad- en loslocatie behoren beveiligd te zijn als de binnendeuren open zijn;	Het is belangrijk om op te merken dat er zich in de verlening van zorg verschillende omstandigheden voordoen waarbij het publiek (patiënten en hun metgezellen) fysiek wordt toegelaten tot zones met grote hoeveelheden gevoelige informatie (bijv. beproevingen in laboratoria waar de workflow kan vereisen dat er informatie van patiënten wordt vergaard in dezelfde ruimte waar op dat moment ook gegevens van eerdere patiënten worden verwerkt; behandelruimtes op de eerste hulp waar metgezellen of

		d) inkomende materialen behoren te worden gecontroleerd en onderzocht op explosieven, chemicaliën of andere gevaarlijke materialen voordat ze vanaf een laad- en loslocatie worden overgebracht; e) inkomende materialen behoren bij binnenkomst op de locatie te worden geregistreerd in overeenstemming met de procedures voor bedrijfsmiddelenbeheer (zie hoofdstuk 8); f) inkomende en uitgaande zendingen behoren, voor zover mogelijk, fysiek te worden gescheiden; g) inkomende materialen behoren te worden gecontroleerd op mogelijke aanwijzingen voor vervalsing tijdens het transport. Indien vervalsing wordt ontdekt behoort dit direct aan beveiligingspersoneel te worden gemeld.	familieleden mogelijk zouden kunnen worden blootgesteld aan aanzienlijke hoeveelheden gevoelige mondelinge en visuele informatie over andere patiënten; computer-/verpleegwerkstations die zich vlakbij de kamers van patiënten bevinden). Die fysieke gebieden binnen de zorg waar gezondheidsinformatie wordt vergaard via gesprekken en waar systemen aanwezig zijn waar gegevens op het scherm worden bekeken, behoren daarom extra toezicht te krijgen. Om te garanderen dat de privacy van patiënten gehandhaafd wordt, is het in de zorg vaak vereist dat er kennisgevingen worden opgehangen in liften, op deuren waarachter gesprekken plaatsvinden en op andere plekken. Dergelijke kennisgevingen dienen als geheugensteuntje dat men het bespreken van patiënten in openbare zones zo veel mogelijk moet beperken.

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang, worden verkleind.	Y	Om apparatuur te beschermen behoren de volgende richtlijnen in overweging te worden genomen: a) apparatuur behoort zo te worden geplaatst dat onnodige toegang tot de werkvloer zo veel mogelijk wordt beperkt; b) informatieverwerkende faciliteiten die gevoelige gegevens behandelen, behoren zorgvuldig te worden gepositioneerd om het risico te verkleinen dat informatie tijdens verwerking door onbevoegde personen wordt ingezien; c) opslagfaciliteiten behoren te worden beveiligd om onbevoegde toegang te voorkomen; d) onderdelen die speciale bescherming nodig hebben, behoren te worden beveiligd zodat het algemene beschermingsniveau dat vereist is, kan worden verlaagd; e) beheersmaatregelen behoren te worden aangenomen om het risico van potentiële fysieke bedreigingen en bedreigingen van buitenaf, bijv. diefstal, brand, explosie, rook, wateroverlast (of uitval van watervoorziening), stof, trilling, chemische reacties, storing in de elektriciteitsvoorziening of in communicatievoorzieningen, elektromagnetische straling en vandalisme, zo laag mogelijk te houden; f) voor eten, drinken en roken in de nabijheid van informatieverwerkende faciliteiten behoren richtlijnen te worden vastgesteld; g) omgevingsomstandigheden zoals temperatuur en vochtigheid behoren te worden gemonitord en gecontroleerd op omstandigheden die de werking van informatieverwerkende faciliteiten negatief kunnen beïnvloeden;	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren eventuele werkstations die toegang bieden tot persoonlijke gezondheidsinformatie, dusdanig te plaatsen dat niet-beoogde inzage of toegang door patiënten en het publiek wordt voorkomen. Medische apparaten die worden gebruikt om gegevens te registreren of rapporteren, kunnen ook speciale overwegingen betreffende beveiliging vereisen met betrekking tot de omgeving waarin ze gebruikt worden en de elektromagnetische emissies die tijdens het gebruik ervan plaatsvinden. Zorginstellingen, met name ziekenhuizen, behoren te garanderen dat de richtlijnen voor plaatsing en bescherming van IT-uitrusting de blootstelling aan dergelijke emissies minimaliseren.

		h) bij alle gebouwen behoort bliksembeveiliging te worden toegepast en op alle inkomende stroom- en communicatieleidingen behoren bliksembeveiligingsfilters te worden geïnstalleerd; i) voor apparatuur in industriële omgevingen behoort de toepassing van speciale beschermingsmiddelen zoals toetsenbordfolie te worden overwogen; j) apparatuur die vertrouwelijke informatie verwerkt, behoort te worden beschermd om het risico van weglekken van informatie door elektromagnetische emanatie zo laag mogelijk te houden.	

A.11.2.2 Nutsvoorzieningen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Y	Nutsvoorzieningen (bijv. elektriciteit, telecommunicatie, watervoorziening, gas, riolering, ventilatie en airconditioning) behoren: a) in overeenstemming te zijn met de technische beschrijving van de fabrikant en de lokale wettelijke eisen; b) regelmatig te worden onderzocht om te beoordelen of hun capaciteit toereikend is voor de groei van het bedrijf en de interactie met andere nutsvoorzieningen; c) regelmatig te worden geïnspecteerd en getest om te waarborgen dat ze correct functioneren; d) zo nodig te worden voorzien van een alarmsysteem om disfunctioneren op te sporen; e) voor zover nodig, te beschikken over meervoudige voeding met een verschillende fysieke route. Noodverlichting en communicatiemiddelen behoren aanwezig te zijn. Nabij nooduitgangen of ruimten waar apparatuur aanwezig is, behoren noodschakelaars en knoppen te zijn waarmee stroom, water, gas of andere voorzieningen kunnen worden uitgeschakeld.	

A.11.2.3 Beveiliging van bekabeling

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	***N***	Met de volgende richtlijnen voor beveiliging van bekabeling behoort rekening te worden gehouden: a) voedings- en telecommunicatieleidingen naar informatieverwerkende faciliteiten behoren, zo mogelijk, ondergronds te lopen, of er behoort adequate alternatieve bescherming te zijn. b) voedingskabels behoren gescheiden te zijn van communicatiekabels om interferentie te voorkomen; c) voor gevoelige of essentiële systemen kunnen de volgende aanvullende beheersmaatregelen worden overwogen: 1) het installeren van gewapende kabelgoten en afgesloten kamers of dozen bij inspectie- en afsluitpunten; 2) het gebruik van elektromagnetische afscherming ter bescherming van de kabels; 3) het initiëren van technische schoonmaakbeurten en fysieke controles op aansluiting van nietgoedgekeurde apparaten op de kabels; 4) beveiligde toegang tot schakelpanelen en kabelruimten.	Gezondheidsorganisaties behoren serieus aandacht te geven aan het afschermen van netwerk- en andere bekabeling in gebieden met hoge emissies uit medische apparaten.

A.11.2.4 Onderhoud van apparatuur

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	***N***	Met de volgende richtlijnen voor onderhoud van apparatuur behoort rekening te worden gehouden: a) apparatuur behoort te worden onderhouden in overeenstemming met de door de leverancier aanbevolen intervallen voor servicebeurten en voorschriften; b) alleen bevoegd onderhoudspersoneel behoort reparaties en onderhoudsbeurten aan apparatuur uit te voeren; c) er behoren registraties te worden bijgehouden van alle vermeende en daadwerkelijke fouten, en van al het preventieve en correctieve onderhoud; d) als apparatuur is ingepland voor onderhoud behoren passende maatregelen te worden geïmplementeerd, waarbij in aanmerking wordt genomen of dit onderhoud wordt uitgevoerd door personeel op locatie of buiten de organisatie; voor zover nodig behoort vertrouwelijke informatie uit de apparatuur te worden verwijderd of het onderhoudspersoneel behoort voldoende betrouwbaar te worden verklaard; e) er behoort te worden voldaan aan alle onderhoudseisen die door verzekeringspolissen zijn opgelegd; f) voordat apparatuur na onderhoud weer in bedrijf wordt gesteld, behoort een inspectie plaats te vinden om te waarborgen dat er niet is geknoeid met de apparatuur en dat deze niet slecht functioneert.	Gezondheidsorganisaties behoren serieus aandacht te geven aan het afschermen van uitrusting in gebieden met hoge emissies uit medische apparaten.

A.11.2.5 Verwijdering van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	***N***	Met de volgende richtlijnen behoort rekening te worden gehouden: a) medewerkers en gebruikers van externe partijen die bevoegd zijn om toe te staan dat bedrijfsmiddelen van de locatie worden meegenomen behoren te worden geïdentificeerd; b) aan de afwezigheid van bedrijfsmiddelen behoren tijdsgrenzen te worden gesteld en er behoort te worden geverifieerd of ze worden teruggebracht; c) voor zover nodig en gepast behoort het meenemen en de terugkeer van bedrijfsmiddelen te worden geregistreerd; d) de identiteit, rol en connectie van iedereen die bedrijfsmiddelen hanteert of gebruikt, behoort te worden gedocumenteerd en deze documenten behoren samen met de apparatuur, informatie of software te worden geretourneerd.	Deze richtlijnen worden afgehandeld in het onderwerp 'telewerken'.

A.11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	***Y***	Het buiten het terrein van de organisatie gebruiken van apparatuur waarop informatie is opgeslagen en die informatie verwerkt, behoort door de directie te worden goedgekeurd. Dit geldt voor apparatuur die eigendom is van de organisatie en voor apparatuur die persoonlijk eigendom is en ten behoeve van de organisatie wordt gebruikt. De volgende richtlijnen behoren in overweging te worden genomen voor het beschermen van apparatuur buiten het terrein van de organisatie: a) apparatuur en media die buiten het terrein worden gebracht behoren niet onbeheerd te worden achtergelaten in openbare ruimten;	Specifiek in de zorgsector bestaat er apparatuur die meegegeven wordt aan patienten. Bv. medische apparatuur voor dialyse, monitoren van hartritme,.. Gezondheidsapps op GSM/Tablet,PC spelen een steeds grotere rol. Men dient hier in de toekomst zeker rekening mee te houden. Zie ook het onderwerp 'telewerken'.

		b) voorschriften van de fabrikant voor het beschermen van de apparatuur behoren te allen tijde in acht te worden genomen, bijv. bescherming tegen blootstelling aan sterke elektromagnetische velden; c) beheersmaatregelen voor locaties buiten het terrein, zoals locaties voor thuiswerken, telewerken en tijdelijke locaties, behoren op basis van een risicobeoordeling te worden vastgesteld, en passende beheersmaatregelen behoren voor zover relevant te worden toegepast, bijv. afsluitbare archiefkasten, 'clear desk'-beleid, toegangsbeveiligingsmaatregelen voor computers en beveiligde communicatie met het kantoor (zie ook de ISO/IEC 27033-reeks); d) als apparatuur buiten het terrein tussen verschillende personen of externe partijen wordt overgedragen, behoort een overzicht te worden bijgehouden dat de bewakingsketen voor de apparatuur definieert, met daarin opgenomen ten minste de namen en organisaties die voor de apparatuur verantwoordelijk zijn. Risico's, bijv. op schade, diefstal of afluisteren, kunnen sterk tussen locaties variëren, en behoren bij het vaststellen van de meest geschikte beheersmaatregelen in overweging te worden genomen.	

A.11.2.7 Veilig verwijderen of hergebruiken van apparatuur

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	Y	Voorafgaand aan verwijdering of hergebruik behoort te worden gecontroleerd of apparatuur opslagmedia bevat. Opslagmedia die vertrouwelijke of door auteursrecht beschermde informatie bevatten, behoren, in plaats van met de standaard 'delete'-functie te worden gewist of te worden geformatteerd, fysiek te worden vernietigd of de informatie behoort te worden vernietigd, verwijderd of overschreven met gebruikmaking van technieken die het onmogelijk maken de oorspronkelijke informatie terug te halen.	

A.11.2.8 Onbeheerde gebruikersapparatuur

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Gebruikers behoren ervoor te zorgen dat onbeheerde apparatuur voldoende beschermd is.	Y	Alle gebruikers behoren op de hoogte te worden gebracht van de beveiligingseisen en de procedures voor het beschermen van onbeheerde apparatuur, en van hun verantwoordelijkheden voor het implementeren van die bescherming. Gebruikers behoren te worden geïnformeerd dat zij: a) actieve sessies na beëindiging afsluiten, tenzij de sessies kunnen worden beveiligd door een geschikte vergrendeling, bijv. een schermbeveiliging die door een wachtwoord wordt beschermd; b) uitloggen uit toepassingen of netwerkdiensten die niet langer nodig zijn; c) computers of mobiele apparatuur beveiligen tegen onbevoegd gebruik door middel van toetsvergrendeling of een vergelijkbaar middel, bijv. toegang via wachtwoord, als de apparatuur niet in gebruik is.	Zie ook 9.3 (Verantwoordelijkheden van gebruikers).

A.11.2.9 'Clear desk'- en 'clear screen'-beleid

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn

Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	Y	Bij het 'clear desk'- en 'clear screen'-beleid behoort rekening te worden gehouden met de informatieclassificatie (zie 8.2), wettelijke en contractuele eisen (zie 18.1) en de bijbehorende risico's en bedrijfscultuur van de organisatie. Met de volgende richtlijnen behoort rekening te worden gehouden: a) gevoelige of essentiële bedrijfsinformatie, bijv. op papier of op elektronische opslagmedia, behoort in een afgesloten ruimte te worden bewaard (idealiter in een kluis, een kast of een andere vorm van beveiligd meubilair) wanneer deze informatie niet vereist is, vooral als het vertrek verlaten is. b) onbeheerde computers en terminals behoren uitgelogd of beschermd te zijn met een scherm- en toetsenbordvergrendeling met wachtwoord, token of vergelijkbare gebruikersauthenticatie; wanneer ze niet worden gebruikt behoren computers en terminals te worden beschermd door toetsvergrendeling, wachtwoorden of andere beheersmaatregelen; c) onbevoegd gebruik van fotokopieerapparaten en andere reproductieapparatuur (bijv. scanners, digitale camera's) behoort te worden voorkomen; d) media die gevoelige of geheime informatie bevatten, behoren na het afdrukken onmiddellijk van printers te worden verwijderd.	Organisaties die gezondheidsinformatie verwerken, behoren bij het bepalen van de verantwoordelijkheden van gebruikers de wettelijk overeengekomen en door leden van organisaties van zorgverleners aanvaarde rechten en ethische verantwoordelijkheden van zorgverleners te respecteren. Zie ook 9.3 (Verantwoordelijkheden van gebruikers).

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	***Y***	Voor bedieningsactiviteiten die samenhangen met informatieverwerkende en communicatiefaciliteiten, zoals de procedures voor het starten en afsluiten van de computer, back-up, onderhoud van apparatuur, behandeling van media, beheer en veiligheid van computerruimte en postverwerking behoren gedocumenteerde procedures te worden opgesteld. In de bedieningsprocedures behoren de bedieningsvoorschriften te zijn opgenomen, onder andere voor: a) back-up (zie 12.3); b) ondersteunings- en escalatiecontacten, waaronder externe ondersteuningscontacten in geval van onverwachte bedienings- of technische moeilijkheden; c) procedures voor het opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen; d) het beheren van audit- en systeemlogbestandinformatie (zie 12.4); e) procedures voor het monitoren van activiteiten.	Vooral voor kritische systemen of toepassingen. Optioneel voor de andere om de maturiteit te verhogen.

A.12.1.2 Wijzigingsbeheer

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, behoren te worden beheerst.	Y	In het bijzonder met de volgende aspecten behoort rekening te worden gehouden: a) identificatie en registratie van significante veranderingen; b) plannen en testen van veranderingen; c) de potentiële impact van dergelijke veranderingen beoordelen, waaronder de impact van de informatiebeveiliging; d) formele goedkeuringsprocedure voor voorgestelde veranderingen; e) verificatie dat is voldaan aan de eisen van informatiebeveiliging; f) communicatie van veranderingsdetails aan alle betrokken personen; g) uitwijkprocedures, waaronder procedures en verantwoordelijkheden voor het afbreken en herstellen van niet-geslaagde veranderingen en onvoorziene gebeurtenissen; h) voorzien in een noodveranderingsproces om veranderingen die nodig zijn om een incident op te lossen snel en beheerst te implementeren (zie 16.1). Verantwoordelijkheden en procedures voor beheer behoren formeel te worden vastgelegd om afdoende beheersing van alle veranderingen te waarborgen. Als de veranderingen hebben plaatsgevonden behoort een auditlogbestand te worden bewaard.	Het is belangrijk om op te merken dat ongepaste, niet afdoende beproefde of onjuiste veranderingen aan het verwerken van persoonlijke gezondheidsinformatie desastreuze gevolgen kunnen hebben voor de zorg voor en veiligheid van patiënten. Het veranderproces behoort de risico's van de verandering expliciet te registreren en te beoordelen. ISO/TS 14441 bevat gedetailleerde richtlijnen voor het testen van de conformiteit van EHR-systemen, waaronder het gebruik van testgegevens. Vooral voor kritische systemen of toepassingen. Optioneel voor de andere om de maturiteit te verhogen.

A.12.1.3 Capaciteitsbeheer

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.	*N*	Capaciteitseisen behoren te worden gedefinieerd, rekening houdend met de bedrijfskritikaliteit van het betrokken systeem. Het systeem behoort te worden afgestemd en gemonitord om de beschikbaarheid en doelmatigheid van systemen te waarborgen en zo nodig te verbeteren. Om problemen vroegtijdig vast te stellen behoren detectiemaatregelen te worden genomen. Prognoses voor toekomstige capaciteitseisen behoren rekening te houden met nieuwe bedrijfs- en systeemeisen en de huidige en verwachte trends in de informatieverwerkende capaciteiten van de organisatie. Speciale aandacht behoort te worden gegeven aan middelen met een lange levertijd of hoge kosten; beheerders behoren daarom het gebruik van belangrijke systeemmiddelen te monitoren. Ze behoren trends in het gebruik te signaleren, vooral in relatie tot bedrijfstoepassingen of beheerinstrumenten voor informatiesystemen. Beheerders behoren deze informatie te gebruiken voor het signaleren en vermijden van potentiële knelpunten en afhankelijkheid van belangrijk personeel die een bedreiging kunnen vormen voor de systeembeveiliging en diensten, en behoren passende actie te plannen. Voldoende capaciteit kan worden verkregen door de capaciteit te verhogen of door de vraag te verlagen. De capaciteitsvraag kan onder meer worden beheerst door: a) verouderde gegevens te verwijderen (schijfruimte); b) toepassingen, systemen, databases of omgevingen buiten gebruik te stellen; c) batchprocessen en -schema's te optimaliseren; d) toepassingslogica of databasevragen te optimaliseren; e) de bandbreedte voor diensten die veel energie verbruiken te weigeren of te beperken als deze niet van overwegend bedrijfsbelang zijn (bijv. videostreaming).	

		Voor systemen die belangrijk zijn voor de missie behoort voor de capaciteit een gedocumenteerd beheersplan te worden overwogen.	

A.12.1.4 Scheiding van ontwikkel-, testen productieomgevingen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	Y	Het scheidingsniveau tussen productie-, test- en ontwikkelomgevingen dat nodig is om operationele problemen te voorkomen behoort te worden geïdentificeerd en geïmplementeerd. Met de volgende aspecten behoort rekening te worden gehouden: a) voor het muteren van software van de ontwikkel- naar de operationele status behoren regels te worden gedefinieerd en gedocumenteerd; b) ontwikkelsoftware en operationele software behoren op verschillende systemen of computerprocessors te draaien en in verschillende domeinen of directory's; c) veranderingen aan productiesystemen en toepassingen behoren te worden getest in een test- of gefaseerde omgeving voordat ze in productiesystemen worden toegepast; d) behoudens uitzonderlijke omstandigheden, behoren tests niet in productiesystemen te worden uitgevoerd; e) compilers, editors en andere ontwikkelinstrumenten of systeemhulpmiddelen behoren, indien ze niet nodig zijn, niet toegankelijk te zijn vanuit productiesystemen; f) gebruikers behoren voor operationele en testsystemen verschillende gebruikersprofielen te gebruiken, en menu's behoren passende identificatieboodschappen te tonen om het risico op fouten te verlagen; g) gevoelige gegevens behoren niet in de omgeving van het testsysteem te worden gekopieerd, tenzij voor het testsysteem equivalente beheersmaatregelen zijn getroffen (zie 14.3).	Elk ziekenhuis dient te definiëren wat men bedoeled met de verschillende omgevingen: • Productie • Acceptatie • Test • Simulatie • Inegratie • Ontwikkeling • … En welke processen er mogen worden uitgevoerd. Het zou bovendien interessant zijn moest men hierover tot een gemeenschappelijk standpunt komen tussen de verschillende instellingen.

A.12.2 Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware

A.12.2.1 Beheersmaatregelen tegen malware

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.	Y	Bescherming tegen malware behoort te zijn gebaseerd op software die malware opspoort en op herstelsoftware, bewustzijn ten aanzien van informatiebeveiliging en passende beheersmaatregelen met betrekking tot systeemtoegang en wijzigingsbeheer. De volgende richtlijnen behoren in acht te worden genomen: a) een formeel beleid vaststellen dat het gebruik van ongeautoriseerde software verbiedt (zie 12.6.2 en 14.2); b) beheersmaatregelen implementeren die het gebruik van ongeautoriseerde software voorkomen of opsporen (bijv. een 'allow' lijst voor toepassingen opstellen); c) beheersmaatregelen implementeren die het gebruik van bekende of verdachte kwaadaardige websites voorkomen of opsporen (bijv. een 'deny' lijst opstellen); d) een formeel beleid vaststellen ter bescherming tegen risico's die samenhangen met het verkrijgen van bestanden en software, hetzij van hetzij via externe netwerken of een	

		ander medium, waarbij wordt aangegeven welke beschermende maatregelen behoren te worden genomen. e) kwetsbaarheden verminderen die kunnen worden geëxploiteerd door malware, bijv. via beheer van technische kwetsbaarheden (zie 12.6); f) regelmatig beoordelingen uitvoeren van de software en gegevensinhoud van systemen die kritische bedrijfsprocessen ondersteunen; de aanwezigheid van niet-goedgekeurde bestanden of ongeautoriseerde wijzigingen behoort formeel te worden onderzocht; g) installeren en regelmatig updaten van software die malware opspoort en van herstelsoftware, waarbij computers en media als voorzorgsmaatregel of routinematig worden gescand; de uitgevoerde scan behoort te omvatten: 1) alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; 2) bijlagen en downloads vóór gebruik op malware scannen; deze scan behoort op verschillende plaatsen te worden uitgevoerd, bijv. op elektronische mailservers, op desktopcomputers en bij de toegang tot het netwerk van de organisatie; 3) internetpagina's op malware scannen; h) ter bescherming tegen malware op systemen procedures en verantwoordelijkheden definiëren, het gebruik ervan trainen, aanvallen van malware melden en herstellen; i) passende bedrijfscontinuïteitsplannen voorbereiden voor het herstel na malwareaanvallen, met inbegrip van de nodige back-up van gegevens en software en herstelprocedures (zie 12.3); j) procedures implementeren om regelmatig informatie te verzamelen, zoals een abonnement op mailinglijsten of het raadplegen van websites die informatie over nieuwe malware geven; k) procedures implementeren om informatie in verband met malware te verifiëren en waarborgen dat waarschuwingsberichten nauwkeurig en informatief zijn; beheerders behoren ervoor te zorgen dat gekwalificeerde bronnen, bijv. goed aangeschreven staande kranten, betrouwbare internetpagina's of leveranciers van antimalwaresoftware, worden geraadpleegd om te differentiëren tussen een hoax en echte malware; alle gebruikers behoren te worden geïnformeerd over het probleem van hoaxen en wat te doen na ontvangst van een hoax; l) omgevingen isoleren als catastrofale impact dreigt.	

A.12.3 Back-up

Doelstelling: Beschermen tegen het verlies van gegevens

A.12.3.1 Back-up van informatie

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Y	Om de eisen van de organisatie voor het back-uppen van informatie, software en systemen te definiëren behoort een back-upbeleid te worden vastgesteld. Het back-upbeleid behoort de eisen voor het bewaren en beschermen te definiëren. Er behoort te worden voorzien in adequate back-upfaciliteiten om te waarborgen dat alle essentiële informatie en software na een calamiteit of na falen van media kan worden hersteld. Bij het opstellen van een back-upplan, behoren de volgende punten in overweging te worden genomen:	

		a) er behoren nauwkeurige en volledige registers van de back-upkopieën en gedocumenteerde herstelprocedures aanwezig te zijn; b) de omvang (bijv. een volledige back-up of alleen van de wijzigingen) en de frequentie van de backups behoren in overeenstemming te zijn met de bedrijfseisen van de organisatie, de beveiligingseisen van de betrokken informatie en de kritikaliteit van de informatie voor de voortzetting van de bedrijfsuitvoering van de organisatie; c) de back-ups behoren in een afgelegen locatie te worden bewaard, op een voldoende afstand om niet te worden beschadigd door een calamiteit op de hoofdlocatie; d) aan back-upinformatie behoort een passend niveau van fysieke en omgevingsbescherming te worden gegeven (zie hoofdstuk 11) consistent met de normen die op de hoofdlocatie worden toegepast; e) back-upmedia behoren regelmatig te worden getest om te waarborgen dat ze betrouwbaar zijn als ze in noodgevallen nodig zijn; dit behoort te worden gecombineerd met een test van de herstelprocedures en van de tijd die voor herstel nodig is. Of de back-upgegevens kunnen worden hersteld, behoort te worden getest op speciaal daarvoor aangewezen testmedia, niet door de originele media te overschrijven omdat het back-up- of herstelproces kan mislukken en onherstelbare schade aan of verlies van gegevens kan veroorzaken; f) in gevallen waarin vertrouwelijkheid belangrijk is, behoren back-ups te worden beschermd door ze te coderen. Bedieningsprocedures behoren de uitvoering van back-ups te monitoren en fouten in geplande backups aan te pakken om de volledigheid van back-ups in overeenstemming met het back-upbeleid te waarborgen. Back-upprocedures voor individuele systemen en diensten behoren regelmatig te worden getest om te waarborgen dat ze voldoen aan de eisen van de bedrijfscontinuïteitsplannen. In geval van kritische systemen en diensten behoren back-upprocedures betrekking te hebben op de informatie, toepassingen en gegevens van alle systemen die nodig zijn om het gehele systeem na een calamiteit te herstellen. Voor belangrijke bedrijfsinformatie behoort de bewaartermijn te worden vastgesteld, rekening houdend met eisen voor archiefkopieën die permanent moeten worden bewaard.	

A.12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

A.12.4.1 Gebeurtenissen registreren

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Y	Logbestanden van gebeurtenissen behoren, voor zover relevant, te bevatten: a) gebruikersidentificaties; b) systeemactiviteiten; c) data, tijdstippen en details van belangrijke gebeurtenissen, bijv. in- en uitloggen. d) identiteit of indien mogelijk de locatie van de apparatuur en de systeemidentificatie; e) registratie van geslaagde en geweigerde pogingen om toegang te verkrijgen tot het systeem;	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren een beveiligd auditverslag aan te maken telkens als een gebruiker via het systeem toegang maakt met persoonlijke gezondheidsinformatie, deze aanmaakt, bijwerkt of archiveert. Het auditverslag behoort op unieke wijze de gebruiker en de persoon waarop de gegevens betrekking hebben (d.w.z. de patiënt), te

		f) registratie van goedgekeurde en geweigerde gegevens en overige pogingen om toegang te verkrijgen tot bronnen van informatie. g) systeemconfiguratieveranderingen; h) gebruik van speciale bevoegdheden; i) gebruik van systeemhulpmiddelen en -toepassingen; j) bestanden die zijn geopend en het type toegang dat is verkregen; k) netwerkadressen en -protocollen; l) alarmen die worden afgegeven door het toegangsbeveiligingssysteem; m) activering en deactivering van beschermingssystemen, zoals antivirussystemen en inbraakdetectiesystemen; n) verslaglegging van transacties die door gebruikers in toepassingen zijn uitgevoerd. Logbestanden van gebeurtenissen vormen de basis van geautomatiseerde monitorsystemen die geconsolideerde rapporten en waarschuwingen over systeembeveiliging kunnen verzamelen.	identificeren, de functie te identificeren die wordt uitgevoerd door de gebruiker (het aanmaken van, toegang maken tot, bijwerken van registraties enz.) en het tijdstip en de datum te vermelden waarop de functie werd uitgevoerd. Als er persoonlijke gezondheidsinformatie wordt bijgewerkt, behoort er een registratie van de voormalige gegevensinhoud en de bijbehorende auditregistratie (d.w.z. wie de gegevens op welke datum heeft ingevoerd) te worden bewaard. Berichtensystemen die worden gebruikt voor het overdragen van berichten die persoonlijke gezondheidsinformatie bevatten, behoren een registratie bij te houden van de overdracht van berichten (die registratie behoort de tijd, datum, herkomst en bestemming van het bericht te bevatten, maar niet de inhoud ervan). De organisatie behoort zorgvuldig de bewaarperiode voor deze auditverslagen te beoordelen en vast te stellen, waarbij met name moet worden gekeken naar klinische beroepsnormen en wettelijke verplichtingen, om het mogelijk te maken dat er onderzoeken worden uitgevoerd en er bewijs van misbruik kan worden geleverd als dit nodig is. De faciliteit voor auditverslagen van het gezondheidsinformatiesysteem behoort te allen tijde operationeel te zijn, terwijl het gezondheidsinformatiesysteem dat gecontroleerd wordt, beschikbaar is voor gebruik. Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie bevatten, behoren te worden uitgerust met faciliteiten voor het analyseren van verslagen en audittrajecten die: a) het mogelijk maken alle systeemgebruikers te identificeren die gedurende een bepaalde periode het zorgdossier van een bepaalde patiënt hebben ingezien of dit gewijzigd hebben; b) het mogelijk maken alle patiënten te identificeren waarvan het zorgdossier gedurende een bepaalde periode is ingezien of gewijzigd. De eisen met betrekking tot het registreren en auditen behoren tot de belangrijkste van alle beveiligingseisen voor het beschermen van persoonlijke gezondheidsinformatie. Deze eisen garanderen rekenschap voor patiënten die hun informatie toevertrouwen aan elektronische registratiesystemen

			voor medische dossiers en zijn tevens een krachtige stimulans voor de gebruikers van dergelijke systemen om het beleid inzake het acceptabele gebruik van deze systemen na te leven. Doeltreffend auditen en registreren kan bijdragen aan het aantonen van misbruik van gezondheidsinformatiesystemen of van persoonlijke gezondheidsinformatie. Deze processen kunnen organisaties en patiënten ook helpen om schadeloosstelling te krijgen van gebruikers die hun toegangsrechten misbruiken. Eisen voor het registreren van gebeurtenissen worden in detail in NEN 7513 en ISO 27789 besproken.

A.12.4.2 Beschermen van informatie in logbestanden

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Y	Beheersmaatregelen behoren gericht te zijn op het beschermen van informatie in logbestanden tegen onbevoegde veranderingen en tegen operationele problemen met de logvoorziening, met inbegrip van: a) veranderingen aan de soorten berichten die worden vastgelegd; b) bewerken of verwijderen van logbestanden; c) overschrijden van de opslagcapaciteit van de media met de logbestanden, waardoor gebeurtenissen niet meer kunnen worden vastgelegd of eerder vastgelegde gebeurtenissen worden overschreven. Als onderdeel van het beleid voor het bewaren van verslagen of in verband met eisen om bewijsmateriaal te verzamelen en bewaren kan het nodig zijn om bepaalde auditlogbestanden te archiveren (zie 16.1.7).	Het is belangrijk om op te merken dat de integriteit van auditregistraties als bewijsmateriaal een essentiële rol kan spelen bij onderzoeken door een patholoog-anatoom, onderzoeken naar medische fouten en andere gerechtelijke of quasigerechtelijke procedures. In dergelijke procedures worden de handelingen van zorgverleners en het tijdstip van gebeurtenissen soms vastgesteld aan de hand van een onderzoek naar veranderingen in en updates van de persoonlijke gezondheidsinformatie van een individu. Met betrekking tot het handhaven van de vertrouwelijkheid en integriteit van medische dossiers en de integriteit en beschikbaarheid van gezondheidsinformatiesystemen, zijn de volgende criteria opgenomen in het document IETF RFC 3881: 'Auditgegevens moeten ten minste even goed worden beveiligd als de onderliggende gegevens en activiteiten die gecontroleerd worden. Dit omvat beheersmaatregelen voor toegang evenals gegevensintegriteits- en herstelfuncties. Dit document erkent de noodzaak van het beleid en de technische methoden om dit te bewerkstellingen, maar schrijft deze niet voor. Het is denkbaar dat er niet-beoogde vormen van gebruik van auditgegevens zijn, bijv. het volgen van de frequentie en aard van het gebruik van systemen voor productiviteitsmaatregelen. In de ASTM-norm E2147-01 staat in paragraaf 5.3.10: "Verbied gebruik om andere redenen dan het handhaven van beveiliging en het opsporen van schendingen van de beveiliging in

			gezondheidsinformatieregistratiesystemen, bijvoorbeeld de audits mogen niet worden gebruikt voor het verkennen van activiteiten- of bewegingsprofielen van werknemers." ’ Het management van auditregistraties behoort de internationale normen over het managen van registraties, ISO 15489, te volgen. Beveiligingseisen voor het archiveren van auditregistraties zijn vergelijkbaar met de beveiligingseisen voor het archiveren van elektronische medische dossiers die in ISO/TS 21547 worden gespecificeerd. Er behoort speciale aandacht te worden besteed aan de beveiliging van gedistribueerde audittrajecten. Waar elektronische medische dossiers over meerdere informatiesystemen verdeeld kunnen zijn en verschillende beveiligingsbeleidsdomeinen beslaan, geldt dit ook voor audittrajecten. De beveiliging van de logische audittrajecten behoort gehandhaafd te worden. Het auditsysteem behoort in afdoende maatregelen te voorzien om te garanderen dat, telkens als het gezondheidsinformatiesysteem operationeel is, dit wordt bijgehouden in het audittraject. Telkens als het audittraject buiten werking of uitgeschakeld is, of door een systeemfout niet werkt, behoort dit in het auditsysteem te worden gedocumenteerd. Het auditsysteem behoort aan te geven of te melden welke audits op een bepaald moment actief of niet actief zijn. Een organisatie die verantwoordelijk is voor het bijhouden van een auditverslag, behoort het bewaarbeleid dat voor de auditregistraties geldt, te definiëren. Het bewaren van de auditregistraties behoort volgens wettelijk voorschriften en relevant beleid te gebeuren. Het bewaren van de auditregistraties behoort de levensduur te ondersteunen van de medische dossiers, gegevens en documenten. Het auditsysteem behoort in voldoende beveiligingsmaatregelen te voorzien om auditverslagen tegen vervalsing te beschermen. Dit behoort in het bijzonder: a) de toegang tot auditregistraties te beveiligen; b) de toegang tot hulpmiddelen voor audits van systemen en audittrajecten te beveiligen om misbruik of compromittering te voorkomen;

			c) alle activiteiten aan het audittraject bij te houden door een beveiligde registratie waarin de tijd, de handeling en de uitvoerende worden vastgelegd; d) alle gelegenheden te documenteren waarop het audittraject buiten werking of uitgeschakeld is, of door een systeemfout niet werkt; e) te melden welke audits op een bepaald moment actief of niet actief zijn. De toegang tot auditgegevens behoort streng gecontroleerd te worden en behoort zelf ook aan controle te worden onderworpen. De toegang behoort plaats te vinden via een gepast informatiesysteem waarmee deze beheersmaatregelen kunnen worden gehandhaafd, in plaats van rechtstreeks toegang tot het audittraject op zich te bieden. Auditfaciliteiten behoren te voorzien in een analyse van het audittraject door gegevensvelden in de registratie, door de datum/tijdsperiode indien van toepassing, hetzij individueel of in combinatie (bijv. alle toegang door gebruiker X, alle 'verwijder'-gebeurtenissen door gebruikers van rol 'Y', alle gebeurtenissen met betrekking tot patiënt 'Z' in de afgelopen maand enz.). In sommige gevallen kan het nodig zijn dat een auditgebruiker in aanvulling op het audittraject toegang heeft tot informatiebronnen, bijvoorbeeld om patronen te ontdekken (bijv. alle zoekopdrachten naar kinderen die zijn uitgevoerd door een gebruiker die geen kinderarts is of niets te maken heeft met kindergeneeskunde). Richtlijnen over het langdurig archiveren en het daarbij garanderen van gegevensintegriteit worden ook gegeven in de documenten IETF RFC 4810 *Long-Term Archive Service Requirements* en IETF RFC 4998 *Evidence Record Syntax (ERS).*

A.12.4.3 Logbestanden van beheerders en operators

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	Y	Houders van een speciaal account zijn mogelijk in staat om de logbestanden op informatieverwerkende faciliteiten die onder hun directe beheer staan te manipuleren. Daarom is het nodig de logbestanden te beschermen en te beoordelen om te handhaven dat speciale gebruikers rekenschap afleggen.	

A.12.4.4 Kloksynchronisatie

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	*Y*	Externe en interne eisen voor weergave, synchronisatie en nauwkeurigheid van tijd behoren te worden gedocumenteerd. Dergelijke eisen kunnen wettelijke, regelgevende of contractuele eisen zijn, naleving van normen of eisen voor interne monitoring. Er behoort een standaard referentietijd voor gebruik binnen de organisatie te worden gedefinieerd. De aanpak van de organisatie om een referentietijd op basis van (een) externe bron(nen) te verkrijgen en hoe interne klokken betrouwbaar te synchroniseren behoren te worden gedocumenteerd en geïmplementeerd.	Het is belangrijk om op te merken dat het tijdstip van gebeurtenissen die elektronisch worden vastgelegd in persoonlijke gezondheidsinformatie en in auditregistraties een essentiële rol kan spelen in processen als onderzoeken door een patholoog-anatoom, onderzoeken naar medische fouten en andere gerechtelijke of quasigerechtelijke procedures, waarbij het essentieel is dat nauwkeurig een klinische volgorde van gebeurtenissen wordt vastgesteld. De kloksynchronisatie is bovendien een absolute vereiste wanneer 'timestamping' gebruikt wordt of dient te worden gebruikt.

A.12.5 Beheersing van operationele software

Doelstelling: De integriteit van operationele systemen waarborgen

A.12.5.1 Software installeren op operationele systemen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	Y	De volgende richtlijnen behoren in overweging te worden genomen om de installatie van software op operationele systemen te beheersen: a) het updaten van de productiesoftware, -toepassingen en -programmabibliotheken behoort alleen te worden uitgevoerd door getrainde beheerders en na de juiste goedkeuring van de directie (zie 9.4.5); b) productiesystemen behoren alleen goedgekeurde uitvoerbare codes te bevatten en geen ontwikkelcodes of compilers; c) toepassingen en besturingssysteemsoftware behoren pas te worden geïmplementeerd na uitgebreide en succesvolle tests; de tests behoren betrekking te hebben op bruikbaarheid, beveiliging, effecten op andere systemen en gebruikersvriendelijkheid, en behoren te worden uitgevoerd op gescheiden systemen (zie 12.1.4); gewaarborgd behoort te worden dat alle corresponderende broncodebibliotheken zijn geüpdatet; d) om alle geïnstalleerde software en systeemdocumentatie te beheersen behoort een configuratiebeheerssysteem te worden toegepast; e) voordat veranderingen worden doorgevoerd behoort een strategie voor het terugdraaien van de veranderingen te zijn vastgesteld; f) van alle updates van besturingsprogrammabibliotheken behoort een auditlogbestand te worden bijgehouden; g) eerdere versies van toepassingssoftware behoren te worden bewaard voor noodgevallen; h) oude versies van software behoren te worden gearchiveerd, samen met alle vereiste informatie en parameters, procedures, configuratiedetails en ondersteunende software, zolang er gegevens in het archief worden bewaard.	Punt h) interpretatie: bij wissel tussen software (andere product bv.) moeten de gegevens van uw vroegere software onder bepaalde omstandigheden toch nog beschikbaar zijn, bv bij een audit.

		Software van leveranciers die in productiesystemen wordt gebruikt behoort te worden onderhouden op een niveau dat door de leverancier wordt ondersteund. Na verloop van tijd zullen softwareleveranciers stoppen met het ondersteunen van oudere softwareversies. De organisatie behoort de risico's van het gebruiken van niet-ondersteunde software te overwegen. Bij beslissingen om te upgraden naar een nieuwe versie behoort rekening te worden gehouden met de bedrijfseisen die gelden voor de verandering en de veiligheid van de versie, d.w.z. de introductie van nieuwe informatiebeveiligingsfunctionaliteit of het aantal en de ernst van informatiebeveiligingsproblemen die zich bij deze versie voordoen. Softwarepatches behoren te worden toegepast als ze kunnen bijdragen aan het verwijderen of verminderen van zwakke plekken in de informatiebeveiliging (zie 12.6). Fysieke of logische toegang behoort alleen te worden verleend aan leveranciers wanneer dit noodzakelijk is voor ondersteuningsdoeleinden en met toestemming van de directie. De activiteiten van de leverancier behoren te worden gemonitord (zie 15.2.1). Computersoftware kan soms steunen op extern geleverde software en modules, die behoren te worden gemonitord en beheerst om onbevoegde veranderingen te vermijden, die zwakke plekken in de beveiliging kunnen introduceren.	

A.12.6 Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen

A.12.6.1 Beheer van technische kwetsbaarheden

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt, behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt, aan te pakken.	Y	Een actuele en volledige inventaris van bedrijfsmiddelen (zie hoofdstuk 8) is een voorwaarde voor een doeltreffend beheer van technische kwetsbaarheden. Tot de specifieke informatie die nodig is om beheer van technische kwetsbaarheden te ondersteunen behoren informatie over de softwareleverancier, versienummers, huidige toepassingsstatus (bijv. welke software is geïnstalleerd op welke systemen) en de persoon of personen in de organisatie verantwoordelijk voor de software. Als reactie op de identificatie van potentiële technische kwetsbaarheden behoort passende en tijdige actie te worden ondernomen. Om een doeltreffend beheerproces voor technische kwetsbaarheden vast te stellen behoren de volgende richtlijnen te worden gevolgd: a) de organisatie behoort de rollen en verantwoordelijkheden in samenhang met het beheer van technische kwetsbaarheden te definiëren en vast te stellen, met inbegrip van het monitoren van de kwetsbaarheden, een risicobeoordeling van de kwetsbaarheden, het installeren van herstelprogramma's (patching), het traceren van bedrijfsmiddelen en de vereiste coördinatieverantwoordelijkheden; b) informatiemiddelen die worden gebruikt om relevante technische kwetsbaarheden te bepalen en om het bewustzijn hierover levend te houden, behoren te worden vastgesteld voor software en andere technologie (op basis van de inventarislijst van bedrijfsmiddelen, zie 8.1.1); deze informatiemiddelen behoren te worden geactualiseerd op basis van veranderingen in de inventarislijst of als andere nieuwe of nuttige middelen zijn gevonden; c) een tijdpad behoort te worden gedefinieerd waarbinnen moet worden gereageerd op aankondigingen van potentieel relevante technische kwetsbaarheden;	Vooral voor kritische systemen of toepassingen. Optioneel voor de andere om de maturiteit te verhogen. Wat zijn de kritische toepassingen ? Er wordt best een lijst opgesteld met de belangrijkste toepassingen die kritisch zijn voor de ziekenhuizen. Hier dient een gemeenschappelijk standpunt te worden ingenomen.

		d) als een potentieel technische kwetsbaarheid is geïdentificeerd, behoort de organisatie de samenhangende risico's en de te ondernemen acties vast te stellen; een dergelijke actie kan patching van kwetsbare systemen inhouden, of het toepassen van andere beheersmaatregelen. e) afhankelijk van hoe urgent een technische kwetsbaarheid moet worden aangepakt behoort de te ondernemen actie te worden uitgevoerd in overeenstemming met de beheersmaatregelen in verband met wijzigingsbeheer (zie 12.1.2) of door responsprocedures voor informatiebeveiligingsincidenten te volgen (zie 16.1.5); f) indien een patch uit een legitieme bron beschikbaar is, behoren de risico's die verbonden zijn aan het installeren van de patch te worden beoordeeld (de risico's die worden gevormd door de kwetsbaarheid behoren te worden vergeleken met het risico van het installeren van de patch); g) patches behoren te worden getest en geëvalueerd voordat ze worden geïnstalleerd om te waarborgen dat ze doeltreffend zijn en niet resulteren in bijverschijnselen die niet kunnen worden getolereerd; indien geen patch beschikbaar is, behoren andere beheersmaatregelen te worden overwogen, zoals: 1) diensten of capaciteiten in verband met de kwetsbaarheid uitschakelen; 2) toegangsbeveiligingsmaatregelen aanpassen of toevoegen, bijv. firewalls, rond de grenzen van netwerken (zie 13.1); 3) vaker monitoren om werkelijke aanvallen op te sporen; 4) bewustzijn omtrent de kwetsbaarheid kweken; h) over alle procedures behoort een auditlogbestand te worden bijgehouden; i) het beheerproces met betrekking tot de technische kwetsbaarheid behoort regelmatig te worden gemonitord en geëvalueerd om de doeltreffendheid en doelmatigheid ervan te waarborgen; j) systemen met een hoog risico behoren eerst te worden aangepakt; k) om gegevens over kwetsbaarheden te communiceren aan de functie die moet reageren op het incident en om te voorzien in uit te voeren technische procedures in geval van een incident, behoort een doeltreffend beheerproces met betrekking tot de technische kwetsbaarheid te worden afgestemd op incidentbeheeractiviteiten; l) een procedure definiëren om de situatie aan te pakken waar een kwetsbaarheid is geïdentificeerd maar waar geen passende tegenmaatregel voorhanden is. In deze situatie behoort de organisatie risico's in verband met de bekende kwetsbaarheid te evalueren en passende opsporings- en corrigerende maatregelen te definiëren.	

A.12.6.2 Beperkingen voor het installeren van software

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Y	De organisatie behoort een strikt beleid te definiëren en ten uitvoer te brengen met betrekking tot de soorten software die gebruikers mogen installeren. Het principe van minimaal voorrecht behoort te worden toegepast. Indien aan gebruikers bepaalde voorrechten worden verleend kunnen zij ook de mogelijkheid hebben om software te installeren. De organisatie behoort vast te leggen welke soorten software mogen worden geïnstalleerd (bijv. updates en beveiligingspatches voor bestaande software) en welke verboden zijn (bijv. software uitsluitend voor persoonlijk gebruik en software waarvan de herkomst met betrekking tot de potentiële kwaadaardigheid onbekend of verdacht is). Deze	

		voorrechten behoren te worden verleend met oog voor de rollen van de betrokken gebruikers.	

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	*N*	De volgende richtlijnen behoren in acht te worden genomen: a) auditeisen voor toegang tot systemen en gegevens behoren met de juiste managers te worden overeengekomen; b) het toepassingsgebied van technische audittests behoort te worden afgesproken en te worden gecontroleerd; c) audittests behoren te worden beperkt tot alleen-lezen-toegang tot software en gegevens; d) toegang anders dan 'alleen lezen' behoort alleen te worden toegelaten voor geïsoleerde kopieën van systeembestanden, die behoren te worden verwijderd als de audit is uitgevoerd, of ze behoren voldoende te worden beschermd indien het verplicht is deze bestanden bij de vereiste auditdocumenten te bewaren; e) eisen voor speciale of extra verwerkingsactiviteiten behoren te worden vastgesteld en overeengekomen; f) audittests die de beschikbaarheid van systemen kunnen beïnvloeden, behoren buiten werkuren plaats te vinden; g) alle toegangshandelingen behoren te worden gemonitord en vastgelegd in een logbestand om een referentietraject te produceren. h)	

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Y	Er behoren beheersmaatregelen te worden geïmplementeerd om de veiligheid van informatie in netwerken te waarborgen en aangesloten diensten tegen onbevoegde toegang te beschermen. Met de volgende aspecten behoort in het bijzonder rekening te worden gehouden: a) er behoren verantwoordelijkheden en procedures voor het beheer van netwerkapparatuur te worden vastgesteld; b) operationele verantwoordelijkheid voor netwerken behoort voor zover van toepassing te worden gescheiden van computerbewerkingen (zie 6.1.2);	

		c) om de vertrouwelijkheid en integriteit van gegevens die via openbare netwerken of draadloze netwerken circuleren te waarborgen en om de aangesloten systemen en toepassingen te beschermen behoren speciale beheersmaatregelen te worden vastgesteld (zie hoofdstuk 10 en 13.2); er kunnen ook speciale beheersmaatregelen vereist zijn om de beschikbaarheid van de netwerkdiensten en aangesloten computers te handhaven; d) om acties die van invloed kunnen zijn op of relevant zijn voor de informatiebeveiliging te kunnen vastleggen en opsporen behoren passende maatregelen voor registreren en monitoren te worden toegepast; e) beheeractiviteiten behoren nauwgezet te worden gecoördineerd, zowel om de dienstverlening voor de organisatie te optimaliseren als om te waarborgen dat beheersmaatregelen consistent in de hele informatieverwerkende infrastructuur worden toegepast; f) systemen in het netwerk behoren te worden geauthentiseerd; g)	

A.13.1.2 Beveiliging van netwerkdiensten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Y	De kundigheid van de aanbieder van de netwerkdienst om de overeengekomen diensten veilig te beheren behoort te worden vastgesteld en regelmatig te worden gemonitord, en het recht om een audit uit te voeren behoort te worden overeengekomen. De beveiligingsprocedures die nodig zijn voor bepaalde diensten, zoals beveiligingskenmerken, dienstverleningsniveaus en beheerseisen, behoren te worden vastgesteld. De organisatie behoort ervoor te zorgen dat aanbieders van netwerkdiensten deze maatregelen implementeren.	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren zorgvuldig te overwegen welke gevolgen het wegvallen van de beschikbaarheid van netwerkdiensten heeft voor de klinische praktijk. Zie ook hoofdstuk 17.

A.13.1.3 Scheiding in netwerken

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	***N***	Een van de methoden om de beveiliging van grote netwerken te beheren is ze te verdelen in gescheiden netwerkdomeinen. De domeinen kunnen worden gekozen op basis van betrouwbaarheidsniveaus (bijv. openbaar toegankelijk domein, bureaubladdomein, serverdomein), naast organisatieafdelingen (bijv. personeelszaken, financiën, marketing) of een combinatie (bijv. serverdomein verbonden met meerdere afdelingen van de organisatie). De scheiding kan tot stand worden gebracht door hetzij fysiek verschillende netwerken, hetzij verschillende logische netwerken te gebruiken (bijv. virtueel particulier netwerken). De perimeter van elk domein behoort goed te worden gedefinieerd. Toegang tussen netwerkdomeinen is toegelaten maar behoort bij de perimeter te worden beheerst door een gateway te gebruiken (bijv. een firewall, een filterende router). De criteria voor het scheiden van netwerken in domeinen, en de toegang die via de gateways wordt toegestaan, behoren te worden gebaseerd op een beoordeling van de beveiligingseisen voor elk domein. De beoordeling behoort in overeenstemming te zijn met het toegangsbeveiligingsbeleid (zie 9.1.1), de toegangseisen, waarde en classificatie van verwerkte informatie en behoort ook rekening te houden met de relatieve kosten en de gevolgen voor de prestaties van het integreren van gatewaytechnologie.	

		Draadloze netwerken vereisen een speciale behandeling in verband met de slecht gedefinieerde netwerkperimeter. Voor gevoelige omgevingen behoort te worden overwogen om elke draadloze toegang te behandelen als externe verbinding en om deze toegang te scheiden van interne netwerken totdat de toegang een gateway is gepasseerd, in overeenstemming met het netwerkcontrolebeleid (zie 13.1.1), alvorens toegang tot interne systemen wordt verleend. De authenticatie, codering en technologie van de netwerktoegangsbeveiliging voor het gebruikersniveau van moderne, op normen gebaseerde draadloze netwerken zijn, indien correct geïmplementeerd, mogelijk voldoende voor directe verbinding met het interne netwerk van de organisatie.	

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

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Y	Bij procedures die moeten worden gevolgd en beheersmaatregelen die moeten worden uitgevoerd bij het gebruik van communicatiefaciliteiten voor informatietransport behoren de volgende punten in overweging te worden genomen: a) procedures die zijn ontworpen ter beveiliging van overgedragen informatie tegen interceptie, kopiëren, wijziging, foutieve routering en vernietiging; b) procedures voor het opsporen van en beschermen tegen malware die kan worden overgebracht door het gebruik van elektronische communicatie (zie 12.2.1); c) procedures ter bescherming van als bijlage gecommuniceerde gevoelige elektronische informatie; d) beleid of richtlijnen die aanvaardbaar gebruik van communicatiefaciliteiten omschrijven (zie 8.1.3); e) verantwoordelijkheden van personeel, van externe partijen en van andere gebruikers om de organisatie niet te compromitteren, bijv. door laster, pesten, aannemen van een valse hoedanigheid, kettingbrieven, onbevoegde inkopen enz. f) gebruik van cryptografische technieken, bijv. om de vertrouwelijkheid, integriteit en authenticiteit van informatie te beschermen (zie hoofdstuk 10); g) richtlijnen voor bewaren en vernietigen van alle bedrijfscorrespondentie, waaronder berichten, in overeenstemming met relevante nationale en lokale wet- en regelgeving; h) beheersmaatregelen en beperkingen die samenhangen met het gebruik van communicatiefaciliteiten, bijv. het geautomatiseerd doorsturen van e-mail naar externe emailadressen; i) personeel adviseren om passende voorzorgsmaatregelen te treffen om geen vertrouwelijke informatie bekend te maken; j) geen berichten die vertrouwelijke informatie bevatten achterlaten op antwoordapparaten omdat deze kunnen worden afgespeeld door onbevoegde personen, op gemeenschappelijke systemen kunnen worden opgeslagen of onjuist kunnen worden opgeslagen als gevolg van foutieve nummerkeuze; k) personeel informeren over problemen in verband met het gebruiken van faxapparatuur of diensten, namelijk:	Organisaties behoren te garanderen dat de beveiliging van dergelijke uitwisseling van informatie het onderwerp is van beleidsontwikkeling en van audits van de naleving ervan (zie hoofdstuk 18). De beveiliging van informatie-uitwisseling kan sterk worden geholpen door gebruik te maken van overeenkomsten over informatie-uitwisseling waarin wordt voorgeschreven welke beheersmaatregelen minimaal moeten worden geïmplementeerd. Er behoort speciale aandacht te worden besteed aan de bruikbaarheid van cryptografische hulpmiddelen. Indien dergelijke hulpmiddelen te complex zijn, zouden gebruikers in de zorg van het gebruik ervan kunnen afzien. Zie ook de zorgspecifieke implementatierichtlijn in 8.2.1. Specifieke richtlijnen over beleid voor het uitwisselen van gezondheidsinformatie zijn te vinden in ISO 22857. Hoewel die internationale norm expliciet verwijst naar grensoverschrijdend verkeer van persoonlijke gezondheidsinformatie (waarbij grenzen in deze context voor grenzen van rechtsgebieden met betrekking tot de zorg staan en niet per se voor landsgrenzen), kunnen veel van de adviezen ervan waar nodig worden aangepast met het oog op de uitwisseling van gegevens van de ene organisatie naar een andere.

		1) onbevoegde toegang tot ingebouwde berichtenboxen om berichten op te vragen; 2) opzettelijk of onbedoeld programmeren van machines waardoor berichten naar bepaalde nummers worden gestuurd; 3) documenten en berichten naar het verkeerde nummer sturen door onjuiste nummerkeuze of door het verkeerde opgeslagen nummer te gebruiken. Bovendien behoort personeel eraan te worden herinnerd dat ze geen vertrouwelijke gesprekken voeren in openbare gebieden of via onbeveiligde communicatiekanalen, in open kantoren en op vergaderlocaties. Diensten op het gebied van informatietransport behoren te voldoen aan relevante wettelijke eisen (zie 18.1).	

A.13.2.2 Overeenkomsten over informatietransport

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	***N***	Overeenkomsten over informatietransport behoren het volgende te bevatten: a) directieverantwoordelijkheden voor het beheersen en notificeren van overdracht, verzending en ontvangst; b) procedures om de traceerbaarheid en onweerlegbaarheid te waarborgen; c) technische minimumeisen voor het verpakken en versturen; d) borgovereenkomsten; e) koerieridentificatienormen; f) verantwoordelijkheden en aansprakelijkheden in geval van informatiebeveiligingsincidenten, zoals verlies van gegevens; g) gebruik van een afgesproken labelsysteem voor gevoelige of essentiële informatie dat waarborgt dat de betekenis van de labels meteen duidelijk is en dat de informatie passend is beschermd (zie 8.2); h) technische normen voor het vastleggen en lezen van informatie en software; i) speciale beheersmaatregelen die vereist zijn om gevoelige informatie te beschermen, zoals cryptografie (zie hoofdstuk 10); j) handhaven van een bewakingsketen voor informatie tijdens verzending; k) acceptabele niveaus van toegangsbeveiliging. Ter bescherming van informatie en fysieke media tijdens overdracht behoren beleidsregels, procedures en normen te worden vastgesteld en gehandhaafd (zie 8.3.3), en hiernaar behoort in overdrachtsovereenkomsten te worden verwezen. De informatiebeveiligingsinhoud van een overeenkomst behoort de gevoeligheid van de desbetreffende bedrijfsinformatie weer te geven.	

A.13.2.3 Elektronische berichten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatie die is opgenomen in elektronische berichten, behoort passend te zijn beschermd.	Y	Overwegingen betreffende informatiebeveiliging van elektronisch berichtenverkeer behoren de volgende aspecten te behelzen:	Organisaties die persoonlijke gezondheidsinformatie door middel van elektronische berichtgeving overdragen, behoren stappen te ondernemen om de vertrouwelijkheid en integriteit van die informatie te

		a) berichten beschermen tegen onbevoegde toegang, wijziging of weigering van dienstverlening in overeenstemming met het classificatieschema dat de organisatie heeft aangenomen; b) correcte adressering en transport van het bericht waarborgen; c) betrouwbaarheid en beschikbaarheid van de dienst; d) wettelijke overwegingen, bijv. eisen voor elektronische handtekeningen; e) toestemming verkrijgen voorafgaand aan het gebruiken van externe openbare diensten zoals instant messaging, sociale netwerken of delen van bestanden; f) hogere niveaus van authenticatie voor het controleren van de toegang vanuit openbaar toegankelijke netwerken.	garanderen. Het is belangrijk om op te merken dat het beveiligen van e-mail en berichten met persoonlijke gezondheidsinformatie die via instant messaging worden verzonden, procedures voor gezondheidspersoneel met zich kan meebrengen die niet kunnen worden opgelegd aan patiënten en het publiek. De uitwisseling van e-mail met persoonlijke gezondheidsinformatie tussen zorgverleners behoort versleuteld te worden verzonden. Hiervoor bestaat een benadering die gepaard gaat met het gebruik van digitale certificaten. Zie ook 18.1.4 voor een bespreking van toestemming voorafgaand aan communicatie buiten de organisatie.

A.13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	***N***	Vertrouwelijkheids- of geheimhoudingsovereenkomsten behoren de eis van bescherming van vertrouwelijke informatie te behandelen binnen juridisch afdwingbare voorwaarden. Vertrouwelijkheids- of geheimhoudingsovereenkomsten zijn van toepassing op externe partijen of medewerkers van de organisatie. Rekening houdend met de aard van de andere partij en de haar toegestane toegang of hantering van vertrouwelijke informatie behoren elementen van de overeenkomst te worden gekozen of toegevoegd. Bij het vaststellen van eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten, behoren de volgende elementen in overweging te worden genomen: a) een definitie van de te beschermen informatie (bijv. vertrouwelijke informatie); b) verwachte looptijd van een overeenkomst, met inbegrip van gevallen waarin de vertrouwelijkheid mogelijk onbeperkt moet worden gehandhaafd; c) vereiste acties als een overeenkomst is beëindigd; d) verantwoordelijkheden en acties van de ondertekenaars betreffende het vermijden van onbevoegd openbaar maken van informatie; e) eigendom van informatie, handelsgeheimen en intellectuele eigendom, en hoe dit zich verhoudt tot de bescherming van vertrouwelijke informatie; f) het toegelaten gebruik van vertrouwelijke informatie en de rechten van de ondertekenaar om informatie te gebruiken; g) het recht om activiteiten waar vertrouwelijke informatie bij betrokken is te auditen en te monitoren; h) procedure voor het notificeren en melden van ongeoorloofde openbaarmaking of lekken van vertrouwelijke informatie; i) voorwaarden voor teruggeven of vernietigen van informatie na beëindiging van de overeenkomst; j) verwachte acties die moeten worden ondernomen in geval van schending van de overeenkomst.	De bovenbedoelde overeenkomst behoort een verwijzing te bevatten naar de straffen die mogelijk zijn als er een schending van het informatiebeveiligingsbeleid wordt geconstateerd.

		Afhankelijk van de eisen van de organisatie betreffende informatiebeveiliging behoren mogelijk nog andere elementen te worden opgenomen in een vertrouwelijkheids- of geheimhoudingsovereenkomst. Vertrouwelijkheids- en geheimhoudingsovereenkomsten behoren te voldoen aan alle toepasselijke wetten en regelgeving voor het rechtsgebied waar zij voor gelden (zie 18.1). Eisen voor vertrouwelijkheids- en geheimhoudingsovereenkomsten behoren periodiek te worden beoordeeld, en als zich veranderingen voordoen die van invloed zijn op deze eisen.	

A.14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

A.14.1 Beveiligingseisen voor informatiesystemen

Doelstelling: Waarborgen dat informatiebeveiliging 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 informatiebeveiligingseisen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Y	Informatiebeveiligingseisen behoren te worden vastgesteld met gebruikmaking van verschillende methoden zoals het afleiden van nalevingseisen van beleidsregels en regelgeving, dreigingsmodellering, beoordelingen van voorvallen of het gebruiken van kwetsbaarheidsdrempels. Resultaten van de identificatie behoren te worden gedocumenteerd en beoordeeld door alle belanghebbenden. Informatiebeveiligingseisen en beheersmaatregelen behoren een afspiegeling te zijn van de waarde van de betrokken informatie voor het bedrijf (zie 8.2) en de potentiële schade voor het bedrijf als gevolg van een gebrek aan adequate beveiliging. Het vaststellen en beheren van informatiebeveiligingseisen en samenhangende processen behoort te worden geïntegreerd in een vroeg stadium van informatiesysteemprojecten. Vroegtijdige overweging van informatiebeveiligingseisen, bijv. in het ontwerpstadium, kan leiden tot oplossingen die doeltreffender en goedkoper zijn. Met betrekking tot informatiebeveiligingseisen behoren ook de volgende aspecten in overweging te worden genomen: a) de vereiste mate van betrouwbaarheid ten opzichte van de beweerde identiteit van gebruikers om authenticatie-eisen voor gebruikers af te leiden; b) procedures voor het verlenen van toegang en autorisatie, voor zakelijke en voor bevoorrechte of technische gebruikers; c) gebruikers en operators informeren over hun plichten en verantwoordelijkheden; d) de vereiste beschermingsbehoeften van de betrokken bedrijfsmiddelen, in het bijzonder met betrekking tot de beschikbaarheid, vertrouwelijkheid en integriteit; e) eisen die zijn afgeleid van bedrijfsprocessen, zoals registreren en monitoren van transacties, eisen voor onweerlegbaarheid; f) eisen die verplicht zijn gesteld door andere beheersmaatregelen met betrekking tot beveiliging, bijv. interfaces voor het registreren en monitoren of systemen voor het opsporen van lekken van gegevens.	ISO/TS 14441 bevat een gedetailleerd pakket functionele privacy- en beveiligingseisen voor EHRsystemen

		Voor toepassingen die diensten verlenen via openbare netwerken of die transacties implementeren, behoren de beheersmaatregelen 14.1.2 en 14.1.3 in overweging te worden genomen. Bij het kopen van producten behoort een formele test- en acquisitieprocedure te worden gevolgd. In de contracten met de leverancier behoren de vastgestelde beveiligingseisen te zijn opgenomen. Als de beveiligingsfunctionaliteit in een voorgesteld product niet voldoet aan de voorgeschreven eis, behoren het geïntroduceerde risico en de daarmee samenhangende beheersmaatregelen te worden heroverwogen voordat het product wordt gekocht. Beschikbare richtlijnen voor de beveiligingsconfiguratie van het product die in overeenstemming zijn gebracht met de uiteindelijke software/dienstverlening van dat systeem behoren te worden geëvalueerd en geïmplementeerd. Criteria voor het accepteren van producten behoren te worden gedefinieerd, bijv. in de zin van hun functionaliteit, wat zekerheid verschaft dat aan de geïdentificeerde beveiligingseisen is voldaan. Voordat producten worden gekocht behoren ze te worden geëvalueerd tegen deze criteria. Om te waarborgen dat de producten geen onacceptabele extra risico's introduceren, behoort extra functionaliteit te worden beoordeeld.	

A.14.1.1.1 Zorgontvangers op unieke wijze identificeren

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
		Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren: a) zeker te stellen dat elke patiënt op unieke wijze kan worden geïdentificeerd binnen het systeem; b) in staat te zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde patiënt zijn aangemaakt, of tijdens een medisch noodgeval.	Het voorzien in zorg in noodgevallen en andere situaties waar toereikende identificatie van patiënten wellicht niet mogelijk is geweest, zal er onvermijdelijk toe leiden dat er meerdere registraties ontstaan voor een en dezelfde patiënt. Binnen elk gezondheidsinformatiesysteem behoort er de nodige capaciteit te zijn om meerdere patiëntregistraties tot één registratie samen te voegen. Dit samenvoegen behoort met de grootst mogelijke zorg te gebeuren en vereist daarom niet alleen personeel dat daarvoor is opgeleid, maar wellicht ook technische hulpmiddelen om betere integratie van informatie uit de oorspronkelijke registraties tot één geheel mogelijk te maken. Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te garanderen dat gegevens op basis waarvan personen kunnen worden geïdentificeerd alleen maar wordt bewaard indien dit nodig is en dat verwijderings-, anonimiserings- en pseudonimiseringstechnieken op gepaste wijze en zo uitgebreid mogelijk worden gebruikt om het risico op onbedoelde openbaarmaking van persoonlijke informatie te minimaliseren.

A.14.1.1.2 Validatie van outputgegevens

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
		Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, behoren te voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de patiënt die wordt behandeld.	Het is nodig een aantal aanvullende belangrijke factoren in aanmerking te nemen. Alvorens te vertrouwen op persoonlijke gezondheidsinformatie die wordt verstrekt door een gezondheidsinformatiesysteem, behoort aan zorgverleners voldoende informatie te worden getoond om te garanderen dat de patiënt die zij behandelen bij de opgevraagde informatie hoort. Het aan een bestaand dossier koppelen van een patiënt is niet altijd een triviale taak. Sommige systemen verhogen de beveiliging door een identificatie aan de hand van een foto op te nemen in elk dossier van een patiënt. Dergelijke verbeteringen kunnen op zich tot privacyproblemen leiden aangezien zij mogelijk het impliciet vastleggen toestaan van gelaatskenmerken zoals ras, die niet als gegevensvelden worden opgenomen. De eisen voor het identificeren van patiënten en de beschikbaarheid van gegevens die worden gebruikt om dit te ondersteunen, kunnen van rechtsgebied tot rechtsgebied verschillen. Er behoort een hoge mate van zorg te worden betracht bij het ontwerpen van gezondheidsinformatiesystemen om te garanderen dat zorgverleners erop kunnen vertrouwen dat het systeem de informatie levert die nodig is om te bevestigen dat elk opgevraagd dossier bij de persoon die onder behandeling is, hoort. Gezondheidsinformatiesystemen behoren controle mogelijk te maken op het volledig zijn van uitdraaien op papier (bijv. ‘pagina 3 van 5’).

A.14.1.2 Toepassingen op openbare netwerken beveiligen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	***N***	Overwegingen betreffende informatiebeveiliging voor toepassingen die zich over openbare netwerken bewegen, behoren de volgende aspecten te bevatten: a) de mate van betrouwbaarheid die beide partijen eisen van elkaars beweerde identiteit, bijv. via authenticatie; b) autorisatieprocedures voor wie de inhoud van belangrijke transactiedocumenten mag goedkeuren, belangrijke transactiedocumenten in circulatie mag brengen of mag ondertekenen; c) bewerkstelligen dat communicatiepartners volledig zijn geïnformeerd over hun bevoegdheden om de dienst te verschaffen of te gebruiken; d) vaststellen van en voldoen aan eisen ten aanzien van vertrouwelijkheid, integriteit, bewijs van verzending en ontvangst van belangrijke documenten en de	Het is belangrijk om te verwijzen naar de zorg die moet worden betracht bij het bepalen of gegevens die betrokken zijn bij elektronische handel en online transacties, persoonlijke gezondheidsinformatie bevatten. Als dat het geval is, behoort deze informatie naar behoren te worden beschermd. Speciale zorg behoort in de zorg uit te gaan naar gegevens in verband met declaraties, medische claims, factuurregels, vorderingen en overige e-commercegegevens waaraan persoonlijke gezondheidsinformatie kan worden ontleend.

		onweerlegbaarheid van contracten, bijv. in samenhang met inschrijvings- en contractprocedures; e) de vereiste mate van vertrouwen in de integriteit van belangrijke documenten; f) de eisen ten aanzien van bescherming van vertrouwelijke informatie; g) de vertrouwelijkheid en integriteit van ordertransacties, betalingsinformatie, gegevens betreffende afleveringsadressen en ontvangstbevestigingen; h) de mate van verificatie die passend is voor controle van betalingsinformatie die door een klant is verstrekt; i) de keuze van de meest geschikte betalingsvorm ter bescherming tegen fraude; j) het vereiste beschermingsniveau om de vertrouwelijkheid en integriteit van orderinformatie te handhaven; k) vermijding van verlies van of vermenigvuldiging van transactie-informatie; l) aansprakelijkheid in verband met frauduleuze transacties; m) eisen met betrekking tot verzekering. Veel van bovengenoemde aspecten kunnen worden aangepakt door toepassing van cryptografische beheersmaatregelen (zie hoofdstuk 10), waarbij rekening wordt gehouden met naleving van wettelijke eisen (zie hoofdstuk 18, zie in het bijzonder 18.1.5 voor wetgeving betreffende cryptografie). Regelingen tussen partners betreffende toepassingen behoren te worden ondersteund door een schriftelijke overeenkomst die beide partijen bindt aan de overeengekomen voorwaarden van de diensten, met inbegrip van afspraken over autorisaties (zie bovenstaand punt b). Eisen betreffende veerkracht tegen aanvallen behoren te worden overwogen; hierbij kan worden gedacht aan eisen ter bescherming van de betrokken toepassingsservers of het waarborgen van de beschikbaarheid van onderlinge netwerkverbindingen die nodig zijn om de dienst te leveren.	

A.14.1.3 Transacties van toepassingen beschermen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatie die deel uitmaakt van transacties van toepassingen, behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	***N***	Overwegingen betreffende informatiebeveiliging voor transacties van toepassingen behoren de volgende aspecten te behelzen: a) het gebruik van elektronische handtekeningen door alle partijen die bij de transactie betrokken zijn; b) alle aspecten van de transactie, d.w.z. waarborgen dat: 1) geheime authenticatie-informatie van gebruikers van alle partijen geldig en geverifieerd is; 2) de transactie vertrouwelijk blijft; 3) de privacy van alle betrokken partijen behouden blijft. c) versleuteling van de communicatiepaden tussen alle betrokken partijen; d) beveiliging van protocollen die worden gebruikt om te communiceren tussen alle betrokken partijen; e) bewerkstelligen dat de opslaglocatie van transactiegegevens zich buiten een publiek toegankelijke omgeving bevindt, bijv. op een opslagplatform op het intranet van de organisatie, en niet wordt bewaard en getoond op een opslagmedium dat direct vanuit internet toegankelijk is;	

		f) als een vertrouwde instantie wordt gebruikt (bijv. voor het uitgeven en onderhouden van digitale handtekeningen of digitale certificaten), beveiliging integreren en inbedden in het gehele beheerproces van certificaten/handtekeningen.	

A.14.1.3.1 Openbaar beschikbare gezondheidsinformatie

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
		Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) behoort te worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie behoort te 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.	

A.14.2 Beveiliging in ontwikkelings- en ondersteunende processen

Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen

A.14.2.1 Beleid voor beveiligd ontwikkelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	Y	Beveiligd ontwikkelen is een eis voor het opbouwen van een beveiligde dienstverlening, architectuur, software en een beveiligd systeem. In een beleid voor beveiligd ontwikkelen behoren de volgende aspecten in overweging te worden genomen: a) beveiliging van de ontwikkelomgeving; b) richtlijnen betreffende beveiliging in de levenscyclus van softwareontwikkeling; 1) beveiliging in de softwareontwikkelmethodologie; 2) beveiligdecoderingsrichtlijnen voor elke programmeertaal die wordt gebruikt. c) beveiligingseisen in de ontwikkelfase; d) beveiligingscontrolepunten binnen de mijlpalen van het project; e) beveiligde informatiecentra; f) beveiliging van de versiecontrole; g) vereiste kennis over toepassingsbeveiliging; h) het vermogen van de ontwikkelaar om kwetsbaarheden te vermijden, te vinden en te repareren. Technieken voor beveiligd programmeren behoren zowel te worden gebruikt voor nieuwe ontwikkelingen als in scenario's voor hergebruik van codes waarvan de normen die voor de ontwikkeling zijn toegepast niet bekend zijn of niet consistent waren met de huidige 'best practices'. Toepassing van beveiligdecoderingsnormen behoort te worden overwogen en indien relevant verplicht te worden gesteld. Ontwikkelaars behoren te worden getraind in het toepassen van codering, en het gebruik behoort te worden geverifieerd door te testen en de codes te beoordelen. Indien ontwikkelactiviteiten worden uitbesteed behoort de organisatie zich ervan te vergewissen dat de externe partij deze regels voor veilig ontwikkelen naleeft (zie 14.2.7).	

A.14.2.2Procedures voor wijzigingsbeheer met betrekking tot systemen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	***N***	Formele procedures voor wijzigingsbeheer behoren te worden gedocumenteerd en afgedwongen om de integriteit van het systeem, de toepassingen en producten te waarborgen, vanaf de vroegste ontwerpstadia tot en met de laatste onderhoudsactiviteiten. De introductie van nieuwe systemen en belangrijke wijzigingen aan bestaande systemen behoort een formeel proces te volgen van documentatie, specificatie, testen, kwaliteitscontrole en beheerde implementatie. Dit proces behoort een risicobeoordeling, een analyse van de gevolgen van wijzigingen en een specificatie van de nodige beveiligingsbeheersmaatregelen te omvatten. Dit proces behoort ook te waarborgen dat bestaande beveiligings- en beheersingsprocedures niet worden gecompromitteerd, dat programmeurs die ondersteunende werkzaamheden uitvoeren alleen toegang krijgen tot die delen van het systeem die zij voor hun werkzaamheden nodig hebben en dat voor elke wijziging formele instemming en goedkeuring is verkregen. Waar mogelijk behoren procedures voor wijzigingsbeheer voor toepassingssoftware en voor de operationele omgeving te worden geïntegreerd (zie 12.1.2). De procedures voor wijzigingsbeheer behoren te omvatten, maar niet beperkt te zijn tot: a) verslaglegging bijhouden van overeengekomen autorisatieniveaus; b) waarborgen dat wijzigingen worden doorgevoerd door bevoegde gebruikers; c) beheersmaatregelen en integriteitsprocedures beoordelen om te waarborgen dat deze niet worden gecompromitteerd door de wijzigingen; d) alle software, informatie, database en hardware identificeren die wijziging behoeven; e) beveiligingskritische codes identificeren en controleren om de waarschijnlijkheid van bekende zwakke plekken in de beveiliging zo gering mogelijk te houden; f) formele goedkeuring voor gedetailleerde voorstellen verkrijgen voor aanvang van de werkzaamheden; g) waarborgen dat bevoegde gebruikers de wijzigingen voorafgaand aan implementatie accepteren; h) waarborgen dat de systeemdocumentatie na elke wijziging wordt geüpdatet en dat oude documentatie wordt gearchiveerd of verwijderd; i) versiebeheer voor alle software-updates uitvoeren; j) een audittraject voor alle wijzigingsverzoeken bijhouden; k) waarborgen dat bedieningsdocumentatie (zie 12.1.1) en gebruikersprocedures indien nodig worden gewijzigd om ze toepasbaar te houden; l) waarborgen dat het implementeren van wijzigingen op het juiste moment plaatsvindt en de betrokken bedrijfsprocessen niet verstoort.	

A.14.2.3 Technische beoordeling van toepassingen na wijzigingen besturingsplatform

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op	N	In deze procedure behoort te zijn opgenomen: a) beoordelen van procedures voor toepassingscontrole en integriteit om te waarborgen dat ze niet zijn gecompromitteerd door de veranderingen aan het besturingsplatform;	Dit is niet altijd mogelijk, daarom wordt dit buiten scope geplaatst. Een voorbeeld is de medische apparatuur waarvan de fabrikant de toegang tot het syteem en/of gegevens verzegelt.

de activiteiten of de beveiliging van de organisatie.		b) waarborgen dat notificatie van veranderingen aan het besturingsplatform tijdig plaatsvindt zodat de aangewezen tests en beoordelingen voorafgaand aan implementatie plaats kunnen vinden; c) bewerkstelligen dat de juiste veranderingen plaatsvinden aan de bedrijfscontinuïteitsplannen (zie hoofdstuk 17).	Cf. Timestamping servers waar de fabrikant de goede werking ervan niet meer gegarandeerd.

A.14.2.4 Beperkingen op wijzigingen aan softwarepakketten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.	***N***	Voor zover mogelijk en haalbaar behoren door aanbieders geleverde softwarepakketten ongewijzigd te worden gebruikt. Als het nodig is een softwarepakket te wijzigen, behoren de volgende punten in overweging te worden genomen: a) het risico dat ingebouwde beheersmaatregelen en integriteitsprocessen gecompromitteerd raken; b) of de toestemming van de verkoper behoort te worden verkregen; c) de mogelijkheid om de vereiste wijzigingen van de aanbieder als standaard programma-updates te verkrijgen; d) de impact als de organisatie verantwoordelijk wordt gehouden voor het toekomstig onderhoud van de software als gevolg van de veranderingen; e) compatibiliteit met andere software die in gebruik is. Indien de veranderingen noodzakelijk zijn, behoort de originele software te worden bewaard en behoren de veranderingen aan een speciaal daarvoor bestemde kopie te worden aangebracht. Er behoort een beheerprocedure voor het updaten van software te worden geïmplementeerd om te bewerkstelligen dat de meest recente goedgekeurde patches en toepassingsupdates bij alle goedgekeurde software zijn geïnstalleerd (zie 12.6.1). Alle veranderingen behoren volledig te worden getest en gedocumenteerd zodat ze zo nodig opnieuw kunnen worden toegepast bij toekomstige software-upgrades. Indien vereist behoren de wijzigingen door een onafhankelijke beoordelingsinstantie te worden getest en gevalideerd.	

A.14.2.5 Principes voor engineering van beveiligde systemen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen. .	Y	Procedures voor de engineering van beveiligde informatiesystemen, gebaseerd op principes voor beveiligde engineering, behoren te worden vastgesteld, gedocumenteerd en toegepast op interne engineeringactiviteiten met betrekking tot informatiesystemen. Beveiliging behoort te worden ontworpen in alle lagen van de architectuur (commercieel, gegevens, toepassingen en technologie), waarbij de behoefte aan informatiebeveiliging behoort te worden afgewogen tegen de behoefte aan toegankelijkheid. Nieuwe technologie behoort te worden geanalyseerd op veiligheidsrisico's en het ontwerp behoort te worden beoordeeld aan de hand van bekende aanvalspatronen. Deze principes en de vastgestelde engineeringprocedures behoren regelmatig te worden beoordeeld om te waarborgen dat ze doelmatig bijdragen aan verbeterde normen voor beveiliging binnen het engineeringproces. Ze behoren ook regelmatig te worden beoordeeld om ervoor te zorgen dat ze actueel blijven in de zin dat ze nieuwe potentiële bedreigingen	

		afwenden en toepasbaar blijven bij verbeteringen die worden toegepast in de technologieën en oplossingen. De voor engineering vastgestelde beveiligingsprincipes behoren indien van toepassing te worden toegepast op uitbestede informatiesystemen via de contracten en andere bindende overeenkomsten tussen de organisatie en de leverancier aan wie de organisatie uitbesteedt. De organisatie behoort te bevestigen dat de strikte toepassing van de beveiligingsprincipes voor engineering vergelijkbaar is met het gebruik in de eigen organisatie.	

A.14.2.6 Beveiligde ontwikkelomgeving

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.	Y	Een beveiligde ontwikkelomgeving omvat personen, processen en technologie die in verband staan met systeemontwikkeling en integratie. Organisaties behoren risico's te beoordelen die samenhangen met individuele verrichtingen betreffende systeemontwikkeling en beveiligde ontwikkelomgevingen vast te stellen voor specifieke verrichtingen op het gebied van systeemontwikkeling, rekening houdend met: a) de gevoeligheid van de gegevens die door het systeem worden verwerkt, opgeslagen en verstuurd; b) toepasselijke externe en interne eisen, bijv. van regelgeving of beleidsregels; c) beheersmaatregelen voor beveiliging die al door de organisatie zijn geïmplementeerd ter ondersteuning van systeemontwikkeling; d) betrouwbaarheid van personeel dat in de omgeving werkt (zie 7.1.1); e) de graad van uitbesteding met betrekking tot systeemontwikkeling; f) de behoefte aan scheiding tussen verschillende ontwikkelomgevingen; g) toegangsbeveiliging voor de ontwikkelomgeving; h) monitoren van veranderingen aan de omgeving en de daarin opgeslagen codes; i) de beheersmaatregel dat back-ups worden bewaard op veilige externe locaties; j) controle over bewegingen van gegevens van en naar de omgeving. Als het beschermingsniveau voor een specifieke ontwikkelomgeving is vastgesteld, behoren organisaties corresponderende processen in veilige ontwikkelprocedures te documenteren en deze beschikbaar te stellen aan alle personen die ze nodig hebben.	

A.14.2.7 Uitbestede softwareontwikkeling

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Y	Als systeemontwikkeling wordt uitbesteed behoren de volgende punten in de gehele externe toeleveringsketen van de organisatie in overweging te worden genomen: a) licentieovereenkomsten, eigendom van de broncode en intellectuele-eigendomsrechten in verband met de uitbestede inhoud (zie 18.1.2); b) contractuele eisen voor beveiligde ontwikkel-, coderings- en testpraktijken (zie 14.2.1); c) acceptatietests voor de kwaliteit en nauwkeurigheid van de leveringen; d) bewijs leveren dat beveiligingsdrempels zijn gebruikt om minimumacceptatieniveaus voor de veiligheid en kwaliteit van privacy toe te passen;	

		e) bewijs leveren dat voldoende tests zijn uitgevoerd om te waken voor de opzettelijke of onbedoelde aanwezigheid van kwaadaardige inhoud op het tijdstip van levering; f) bewijs leveren dat voldoende tests zijn uitgevoerd om te waken voor de aanwezigheid van bekende kwetsbaarheden; g) regelingen voor het deponeren van de broncode, bijv. indien de broncode niet langer beschikbaar is; h) contractueel recht om ontwikkelprocessen en beheersmaatregelen te auditen; i) doeltreffende documentatie van de gebouwde omgeving die wordt gebruikt om af te leveren producten te creëren; j) de organisatie blijft verantwoordelijk voor naleving van toepasselijke wetten en verificatie van de doelmatigheid van de controle	

A.14.2.8 Testen van systeembeveiliging

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Y	Tijdens de ontwikkelprocessen zijn voor nieuwe en geactualiseerde systemen uitvoerige tests en verificatie nodig, met inbegrip van het opstellen van een gedetailleerd schema van activiteiten en tests van inputs en verwachte outputs onder diverse omstandigheden. Voor interne ontwikkelactiviteiten behoren dergelijke tests in eerste instantie te worden uitgevoerd door het ontwikkelteam. Vervolgens behoren onafhankelijke tests te worden uitgevoerd (zowel voor interne als voor uitbestede ontwikkelactiviteiten) om te bewerkstelligen dat het systeem uitsluitend werkt zoals voorzien (zie 14.1.1 en 14.2.9). De omvang van het testen behoort in verhouding te staan tot de belangrijkheid en de aard van het systeem.	

A.14.2.9 Systeemacceptatietests

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Y	Het uitvoeren van systeemacceptatietests behoort mede het testen van informatiebeveiligingseisen te omvatten (zie 14.1.1 en 14.1.2) en het volgen van een veilige werkwijze voor systeemontwikkeling (zie 14.2.1). De tests behoren ook te worden uitgevoerd op ontvangen componenten en geïntegreerde systemen. Organisaties kunnen geautomatiseerde instrumenten inzetten zoals instrumenten om codes te analyseren of om op kwetsbaarheden te scannen, en behoren het herstel van beveiligingsgerelateerde tekortkomingen te verifiëren. Tests behoren te worden uitgevoerd in een realistische testomgeving om te bewerkstelligen dat het systeem geen kwetsbaarheden introduceert in de omgeving van de organisatie en dat de tests betrouwbaar zijn.	De omvang en nauwgezetheid van die tests behoren te worden ingeschaald op een niveau dat bij de geïdentificeerde risico's van de verandering past. Zie ook 12.1.2.

A.14.3 Testgegevens

Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt

A.14.3.1 Bescherming van testgegevens

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	Y	Het voor testdoeleinden gebruiken van operationele databases met persoonsgegevens of enige andere vertrouwelijke informatie behoort te worden vermeden. Indien persoonsgegevens of anderszins vertrouwelijke informatie wordt gebruikt voor testdoeleinden, behoren alle gevoelige details en inhoud te worden beschermd door deze te verwijderen of te wijzigen (zie ISO/IEC 29101). De volgende richtlijnen behoren te worden toegepast om operationele gegevens te beschermen die voor testdoeleinden worden gebruikt: a) de toegangsbeveiligingsprocedures die gelden voor besturingssystemen behoren ook te gelden voor testsystemen; b) voor elke keer dat besturingsinformatie naar een testomgeving wordt gekopieerd, behoort een afzonderlijke autorisatie te worden verkregen; c) besturingsinformatie behoort onmiddellijk na voltooiing van het testen uit een testomgeving te worden verwijderd; d) van het kopiëren en gebruiken van besturingsinformatie behoort verslaglegging te worden bijgehouden om in een audittraject te voorzien.	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren daadwerkelijke persoonlijke gezondheidsinformatie niet als testgegevens te gebruiken. ISO/TS 14441 bevat gedetailleerde richtlijnen over het testen van de conformiteit van EHR-systemen, waaronder het gebruik van testgegevens.

A.15 Leveranciersrelaties

A.15.1 Informatiebeveiliging in leveranciersrelaties

Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers

A.15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	Y	De organisatie behoort beheersmaatregelen voor informatiebeveiliging vast te stellen en verplicht te stellen om specifiek de toegang van de leverancier tot de informatie van de organisatie beleidsmatig aan te pakken. Deze beheersmaatregelen behoren betrekking te hebben op de door de organisatie te implementeren processen en procedures, en op de processen en procedures waarvan de organisatie behoort te eisen dat de leverancier deze implementeert, met inbegrip van: a) vaststellen en documenteren van de soorten leveranciers, bijv. IT-diensten, logistieke voorzieningen, financiële diensten, IT-infrastructuurcomponenten waarvan de organisatie de toegang tot de informatie wil toestaan; b) een gestandaardiseerd proces en gestandaardiseerde levenscyclus voor het beheren van leveranciersrelaties; c) definiëren van de soorten informatietoegang die verschillende soorten leveranciers wordt toegestaan, en de toegang monitoren en controleren; d) een minimum aan informatiebeveiligingseisen voor elk soort informatie en elk soort toegang dat dient als basis voor individuele leveranciersovereenkomsten, gebaseerd op de bedrijfsbehoeften en -eisen van de organisatie en haar risicoprofiel; e) processen en procedures voor het monitoren van de naleving van vastgestelde informatiebeveiligingseisen voor elk soort leverancier en elk soort toegang, met inbegrip van beoordeling van derden en productvalidatie; f) beheersmaatregelen betreffende nauwkeurigheid en volledigheid ter waarborging van de integriteit van de informatie of informatieverwerking die elke partij biedt;	Risicobeoordeling is essentieel voor doeltreffend management van de toegang door derden tot systemen die gezondheidsinformatie, met name persoonlijke gezondheidsinformatie, bevatten. De rechten van patiënten behoren te worden beschermd, zelfs wanneer een externe partij met potentiële toegang tot persoonlijke gezondheidsinformatie zich in een ander rechtsgebied bevindt dan het rechtsgebied dat van kracht is voor de patiënt of de gezondheidsorganisatie.

		g) soorten verplichtingen die van toepassing zijn op leveranciers om de informatie van de organisatie te beschermen; h) omgaan met incidenten en noodsituaties die verband houden met toegang voor leveranciers met inbegrip van verantwoordelijkheden van zowel de organisatie als van de leveranciers; i) regelingen voor flexibiliteit en, zo nodig voor herstel en noodsituaties om de beschikbaarheid te waarborgen van de informatie of de informatieverwerking die door elk van de partijen wordt geboden; j) bewustzijnstraining voor het personeel van de organisatie dat betrokken is bij acquisitie met betrekking tot toepasselijke beleidsregels, processen en procedures; k) bewustzijnstraining voor het personeel van de organisatie dat contacten onderhoudt met personeel van de leverancier betreffende passende regels van betrokkenheid en gedrag, gebaseerd op het type leverancier en het soort toegang dat de leverancier heeft tot systemen en informatie van de organisatie; l) voorwaarden waarop informatiebeveiligingseisen en beheersmaatregelen zullen worden gedocumenteerd in een overeenkomst die door beide partijen wordt ondertekend; m) beheren van de nodige transities van informatie, informatieverwerkende faciliteiten en al het andere dat moet overgaan, en waarborgen dat informatiebeveiliging tijdens de gehele transitieperiode wordt gehandhaafd.	

A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Alle relevante informatiebeveiligingseisen behoren te 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.	Y	Leveranciersovereenkomsten behoren te worden vastgesteld en gedocumenteerd om te waarborgen dat er geen misverstand tussen de organisatie en de leverancier bestaat ten aanzien van de verplichtingen van beide partijen om te voldoen aan relevante informatiebeveiligingseisen. Overwogen behoort te worden om de volgende voorwaarden in de overeenkomsten op te nemen om te voldoen aan de vastgestelde informatiebeveiligingseisen: a) omschrijving van de informatie die moet worden verschaft of toegankelijk moet worden en methoden om de informatie te verschaffen of toegankelijk te maken; b) classificatie van de informatie in overeenstemming met het classificatieschema van de organisatie (zie 8.2); zo nodig ook mapping tussen het eigen schema van de organisatie en het schema van de leverancier; c) wettelijke en regelgevende eisen, met inbegrip van gegevensbescherming, rechten van intellectuele eigendom en auteursrecht, en een beschrijving van hoe wordt gewaarborgd dat eraan wordt voldaan; d) verplichting van elke contractuele partij om een overeengekomen aantal beheersmaatregelen te implementeren, waaronder toegangsbeveiliging, prestatiebeoordeling, monitoren, rapporteren en auditen; e) de regels van aanvaardbaar gebruik van informatie, met inbegrip van onaanvaardbaar gebruik indien noodzakelijk; f) hetzij een expliciete lijst van leverancierspersoneel dat geautoriseerde toegang heeft of bevoegd is informatie van de organisatie te ontvangen, hetzij procedures of voorwaarden voor autorisatie en het intrekken van de autorisatie, tot toegang tot of ontvangst van informatie van de organisatie door leverancierspersoneel.	Het managen van dienstverlening door derden wordt sterk vereenvoudigd als er een formele overeenkomst wordt gesloten die aangeeft welke beheersmaatregelen er minimaal moeten worden geïmplementeerd.

		g) beleidsregels betreffende informatiebeveiliging die relevant zijn voor het specifieke contract; h) eisen voor incidentbeheer en -procedures (in het bijzonder notificatie en samenwerking tijdens herstel van het incident); i) trainings- en bewustzijnseisen voor specifieke procedures en informatiebeveiligingseisen, bijv. voor incidentresponsprocedures, autorisatieprocedures; j) relevante regelgeving voor onderaanneming, met inbegrip van de beheersmaatregelen die moeten worden geïmplementeerd; k) relevante overeenkomstpartners, met inbegrip van een contactpersoon voor aangelegenheden betreffende informatiebeveiliging; l) indien relevant, screeningeisen voor leverancierspersoneel, met inbegrip van verantwoordelijkheden voor het uitvoeren van de screening en notificatieprocedures indien de screening niet is voltooid of de resultaten aanleiding geven tot twijfel of bezorgdheid; m) het recht om de processen en beheersmaatregelen van de leverancier in verband met de overeenkomst te auditen; n) procedures voor het oplossen van defecten en conflicten; o) verplichting van de leverancier om periodiek een onafhankelijk rapport te verstrekken over de doeltreffendheid van beheersmaatregelen, en overeenkomst over tijdige correctie van relevante kwesties die in het rapport aan de orde worden gesteld; p) verplichting van de leverancier om te voldoen aan de beveiligingseisen van de organisatie.	

A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Overeenkomsten met leveranciers behoren eisen te 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.	Y	Overwogen behoort te worden de volgende onderwerpen op te nemen in leveranciersovereenkomsten betreffende beveiliging van de toeleveringsketen: a) informatiebeveiligingseisen definiëren die gelden voor acquisitie van producten of diensten op het gebied van informatie- en communicatietechnologie naast de algemene informatiebeveiligingseisen voor leveranciersrelaties; b) met betrekking tot diensten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers de beveiligingseisen van de organisatie in de gehele toeleveringsketen bekendmaken indien leveranciers delen van diensten op het gebied van informatie- en communicatietechnologie die zij aan de organisatie leveren, uitbesteden; c) met betrekking tot producten op het gebied van informatie- en communicatietechnologie, eisen dat leveranciers passende beveiligingspraktijken in de gehele toeleveringsketen bekendmaken indien deze producten componenten bevatten die van andere leveranciers worden betrokken; d) een monitorproces en aanvaardbare methoden implementeren om te valideren dat geleverde producten en diensten op het gebied van informatie- en communicatietechnologie in overeenstemming zijn met verklaarde beveiligingseisen; e) een proces implementeren voor het vaststellen van componenten van producten of diensten die essentieel zijn voor het handhaven van de functionaliteit en daardoor verhoogde aandacht en toezicht vereisen als deze buiten de organisatie worden	

		gebouwd, in het bijzonder indien de eindleverancier delen van componenten van producten of diensten aan andere leveranciers uitbesteedt; f) zekerheid verkrijgen dat essentiële componenten en de herkomst ervan in de toeleveringsketen kunnen worden nagespeurd; g) zekerheid verkrijgen dat de geleverde producten op het gebied van informatie- en communicatietechnologie functioneren zoals voorzien zonder onverwachte of ongewenste verschijnselen; h) regels definiëren voor het delen van informatie met betrekking tot de toeleveringsketen en potentiële kwesties en compromissen tussen de organisatie en leveranciers; i) specifieke processen implementeren voor het beheren van de levenscyclus en de beschikbaarheid van de componenten van de informatie- en communicatietechnologie en samenhangende beveiligingsrisico's. Hiertoe behoort het beheren van de risico's van componenten die niet langer beschikbaar zijn doordat leveranciers niet meer bestaan of doordat leveranciers deze componenten niet meer leveren in verband met verbeterde technologie.	

A.15.2 Beheer van dienstverlening van leveranciers

Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven

A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	Y	Het monitoren en beoordelen van dienstverlening van leveranciers behoort te waarborgen dat aan de voorwaarden van informatiebeveiliging wordt voldaan, en dat incidenten en problemen betreffende informatiebeveiliging op de juiste manier worden behandeld. Hiertoe behoort een proces voor het beheer van de dienstverlening te bestaan betreffende de relatie tussen de organisatie en de leverancier om: a) de prestatieniveaus van de dienstverlening te monitoren om naleving van de overeenkomsten te verifiëren; b) de rapporten over de dienstverlening die zijn opgesteld door de leverancier te beoordelen, en regelmatig voortgangsbesprekingen te regelen voor zover door de overeenkomsten vereist; c) audits van leveranciers uit te voeren, indien beschikbaar tezamen met de beoordeling van rapporten van onafhankelijke auditoren, en vastgestelde kwesties op te volgen; d) informatie te verstrekken over informatiebeveiligingsincidenten en deze informatie te beoordelen voor zover vereist door de overeenkomsten en ondersteunende richtlijnen en procedures; e) audittrajecten van leveranciers en verslagen van informatiebeveiligingsgebeurtenissen, operationele problemen, weigeringen, opsporing van storingen en onderbrekingen in verband met de geleverde dienst te beoordelen; f) vastgestelde problemen op te lossen en te beheren; g) informatiebeveiligingsaspecten van de relaties van de leverancier met zijn eigen leveranciers te beoordelen; h) te bewerkstelligen dat de leverancier voldoende capaciteit voor de diensten onderhoudt samen met werkbare plannen die zijn ontworpen om te waarborgen dat de	Zie ook de zorgspecifieke implementatierichtlijn in 15.1.2.

		overeengekomen continuïteitsniveaus van de dienstverlening na grote storingen of calamiteiten in de dienstverlening worden onderhouden (zie hoofdstuk 17). De verantwoordelijkheid voor het beheer van leveranciersrelaties behoort te worden toegekend aan een daarvoor aangewezen persoon of dienstverleningsbeheerteam. De organisatie behoort verder ervoor te zorgen dat leveranciers verantwoordelijkheden toewijzen voor het beoordelen van de naleving en het dwingend uitvoeren van de eisen van de overeenkomsten. Om te monitoren dat de eisen van de overeenkomst, in het bijzonder de informatiebeveiligingseisen, worden nagekomen, behoren voldoende technische vaardigheden en middelen beschikbaar te worden gesteld. Als tekortkomingen in de dienstverlening worden waargenomen behoort passende actie te worden ondernomen. De organisatie behoort voldoende algehele controle over en zicht te houden op alle beveiligingsaspecten betreffende gevoelige of essentiële informatie of informatieverwerkende faciliteiten die toegankelijk zijn voor, worden verwerkt of beheerd door een leverancier. De organisatie behoort via een gedefinieerde rapportageprocedure zicht te houden op beveiligingsactiviteiten zoals wijzigingsbeheer, vaststellen van kwetsbaarheden en rapporteren van en respons op informatiebeveiligingsincidenten.	

A.15.2.2 Beheer van veranderingen in dienstverlening van leveranciers

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Y	De volgende aspecten behoren in overweging te worden genomen: a) veranderingen in leveranciersovereenkomsten; b) veranderingen die door de organisatie zijn aangebracht ter implementatie van: 1) verbeteringen van de huidige aangeboden dienstverlening; 2) ontwikkelingen van nieuwe toepassingen en systemen; 3) wijzigingen in of updates van beleid en procedures van de organisatie; 4) nieuwe of gewijzigde beheersmaatregelen om informatiebeveiligingsincidenten op te lossen en om de veiligheid te verbeteren. c) veranderingen in diensten van de leverancier ter implementatie van: 1) veranderingen en verbeteringen van netwerken; 2) gebruik van nieuwe technologieën; 3) aanvaarding van nieuwe producten of nieuwe versies/uitgaven; 4) nieuwe ontwikkelinstrumenten en omgevingen; 5) veranderingen in fysieke locatie van dienstverleningsfaciliteiten; 6) verandering van leverancier; 7) onderaanneming bij een andere leverancier.	Zie ook de zorgspecifieke implementatierichtlijn in 15.1.2.

A.16 Beheer van informatiebeveiligingsincidenten

A.16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging

A.16.1.1 Verantwoordelijkheden en procedures

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn

Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Y	Met betrekking tot het beheer van informatiebeveiligingsincidenten behoren de volgende richtlijnen voor directieverantwoordelijkheden en -procedures in overweging te worden genomen: a) er behoren directieverantwoordelijkheden te worden vastgesteld om te bewerkstelligen dat de volgende procedures adequaat binnen de organisatie worden ontwikkeld en gecommuniceerd: 1) procedures voor incidentresponsplanning en -voorbereiding; 2) procedures voor het monitoren, opsporen, analyseren en rapporteren van informatiebeveiligingsgebeurtenissen en -incidenten; 3) procedures voor de verslaglegging van beheeractiviteiten betreffende incidenten; 4) procedures voor het omgaan met forensisch bewijs; 5) procedures voor het beoordelen van en besluitvorming over informatiebeveiligingsgebeurtenissen en beoordeling van zwakke plekken in de informatiebeveiliging; 6) responsprocedures met inbegrip van procedures voor escalatie, beheerst herstel van een incident en communicatie aan in- en externe personen of organisaties. b) vastgestelde procedures behoren te bewerkstelligen dat: 1) competent personeel de kwesties behandelt die verband houden met informatiebeveiligingsincidenten binnen de organisatie; 2) een contactpunt voor het opsporen en rapporteren van beveiligingsincidenten wordt geïmplementeerd; 3) passende contacten worden onderhouden met instanties, externe belangengroepen of fora die aangelegenheden behandelen die verband houden met informatiebeveiligingsincidenten. c) rapportageprocedures behoren de volgende aspecten te omvatten: 1) formulieren voorbereiden voor het rapporteren van informatiebeveiligingsgebeurtenissen ter ondersteuning van de rapportageactie en om te bevorderen dat de rapporterende persoon aan alle nodige acties denkt die in geval van een informatiebeveiligingsgebeurtenis moeten worden verricht; 2) de procedures die in geval van een informatiebeveiligingsgebeurtenis moeten worden uitgevoerd, bijv. onmiddellijk alle details noteren, zoals aard van niet-naleving of overtreding, optredende storing, berichten op het scherm, en onmiddellijk rapporteren aan het contactpunt en alleen gecoördineerde actie ondernemen; 3) verwijzing naar een vastgestelde disciplinaire formele procedure voor het omgaan met medewerkers die beveiligingsovertredingen begaan; 4) passende feedbackprocedures om te bewerkstelligen dat de personen die informatiebeveiligingsgebeurtenissen melden, worden geïnformeerd over de resultaten nadat de kwestie is behandeld en afgesloten. De doelstellingen voor het beheer van informatiebeveiligingsincidenten behoren met de directie te worden overeengekomen en er behoort te worden gewaarborgd dat de personen die verantwoordelijk zijn voor het beheer van informatiebeveiligingsincidenten op de hoogte zijn van de prioriteiten van de organisatie voor het behandelen van informatiebeveiligingsincidenten.	

A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Y	Alle medewerkers en contractanten behoren bewust te worden gemaakt van hun verantwoordelijkheid om informatiebeveiligingsgebeurtenissen zo snel mogelijk te rapporteren. Zij behoren ook te worden geïnformeerd over de procedure voor het rapporteren van informatiebeveiligingsgebeurtenissen en het contactpunt waaraan de gebeurtenissen behoren te worden gerapporteerd. Met betrekking tot het rapporteren van informatiebeveiligingsgebeurtenissen behoort rekening te worden gehouden met de volgende situaties: a) niet-doeltreffende beveiligingsbeheersmaatregelen; b) schending van informatie-integriteit, vertrouwelijkheid of aanwezige verwachtingen; c) menselijke fouten; d) niet-naleving van beleidsregels of richtlijnen; e) schending van fysieke beveiligingsregelingen; f) onbeheerste systeemveranderingen; g) storingen in soft- of hardware; h) overtredingen van de toegangsregeling.	Er is een tendens in gezondheidsorganisaties om informatiebeveiligingsincidenten kunstmatig van andere soorten incidenten te scheiden, zowel wat betreft de afhandeling ervan als het rapporteren erover. Met het oog op het feit dat een inbraak zou kunnen hebben geleid tot de diefstal van IThardware (hetgeen tot een schending van de vertrouwelijkheid leidt) of dat er brand zou kunnen zijn gesticht om het misbruik van IT-apparatuur te verhullen, of dat geïdentificeerd misbruik of foutief gebruik van het systeem klinische gevolgen zou kunnen hebben gehad, behoort er een informatiebeveiligingsbeoordeling te worden uitgevoerd van al dergelijke incidenten of van een representatief incident om de doeltreffendheid van gevestigde beheersmaatregelen en van de risicobeoordeling die tot de implementatie ervan heeft geleid verder te evalueren.

A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie, behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Y	Alle medewerkers en contractanten behoren deze zaken zo snel mogelijk aan het contactpunt te rapporteren om informatiebeveiligingsincidenten te voorkomen. Het rapporteringsmechanisme behoort zo eenvoudig, toegankelijk en beschikbaar te zijn als mogelijk is.	

A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Y	Het contactpunt behoort elke informatiebeveiligingsgebeurtenis te beoordelen op basis van de overeengekomen classificatieschema voor gebeurtenissen en incidenten betreffende informatiebeveiliging, en te besluiten of de gebeurtenis behoort te worden geclassificeerd als informatiebeveiligingsincident. Classificeren en prioriteren van incidenten kan helpen de impact en omvang van een incident te bepalen. In gevallen waarin de organisatie beschikt over een responsteam voor informatiebeveiligingsincidenten (ISIRT), kunnen de beoordeling en het besluit worden doorgestuurd naar het ISIRT voor bevestiging of herbeoordeling. Resultaten van de beoordeling en het besluit behoren in detail in een verslag te worden vastgelegd ten behoeve van toekomstige verwijzing en verificatie.	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren te beoordelen of de informatiebeveiligingsgebeurtenis persoonlijke gezondheidsinformatie betrof.

A.16.1.5 Respons op informatiebeveiligingsincidenten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Y	Op informatiebeveiligingsincidenten behoort te worden gereageerd door een aangewezen contactpunt en andere relevante personen van de organisatie of externe partijen (zie 16.1.1). De respons behoort de volgende aspecten te omvatten: a) zo snel mogelijk na de gebeurtenis bewijs verzamelen; b) indien vereist, forensische analyse van de informatiebeveiliging uitvoeren (zie 16.1.7); c) escaleren indien vereist; d) bewerkstelligen dat alle betrokken responsactiviteiten op de juiste manier worden vastgelegd voor latere analyse; e) het bestaan van het informatiebeveiligingsincident of relevante details daarvan communiceren aan andere in- en externe personen of organisaties met een 'need-to-know'; f) behandelen van de zwakke plek(ken) in de informatiebeveiliging waarvan is vastgesteld dat deze het incident heeft/hebben veroorzaakt of eraan heeft/hebben bijgedragen; g) het incident formeel afsluiten en verslaglegging bijhouden zodra het incident met succes is behandeld. Om de bron van het incident te identificeren behoort postincidentanalyse plaats te vinden.	

A.16.1.6 Lering uit informatiebeveiligingsincidenten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Y	Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gemonitord. De informatie die is verkregen uit de evaluatie van informatiebeveiligingsincidenten behoort te worden gebruikt om terugkerende of ingrijpende incidenten te identificeren.	

A.16.1.7 Verzamelen van bewijsmateriaal

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Y	Bij het omgaan met bewijs ten behoeve van disciplinaire en wettelijke actie behoren interne procedures te worden ontwikkeld en gevolgd. In het algemeen behoren deze bewijsprocedures processen in te houden voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs in overeenstemming met de verschillende soorten media, apparaten en de status van de apparaten, bijv. in- of uitgeschakeld. De procedures behoren rekening te houden met de: a) bewakingsketen; b) veiligheid van bewijs; c) veiligheid van personeel; d) rollen en verantwoordelijkheden van het betrokken personeel; e) competentie van personeel; f) documentatie;	Het kan voor organisaties die persoonlijke gezondheidsinformatie verwerken, nodig zijn aandacht te geven aan de implicaties van het verzamelen van bewijs om medische fouten aan te tonen en aandacht te geven aan interjurisdictionele eisen als gezondheidsinformatiesystemen van buiten de grenzen van het eigen rechtsgebied toegankelijk zijn.

		g) instructie. Indien beschikbaar, behoort certificatie of andere relevante methoden om personeel en middelen te kwalificeren te worden gezocht om de waarde van het verkregen bewijs te versterken. Forensisch bewijs kan grenzen van organisaties of rechtsgebieden overschrijden. In zulke gevallen behoort te worden gewaarborgd dat de organisatie het recht heeft de vereiste informatie als forensisch bewijs te verzamelen. De eisen van verschillende rechtsgebieden behoren ook in aanmerking te worden genomen om de kans zo groot mogelijk te maken dat het bewijs wordt toegelaten in de relevante rechtsgebieden	

A.17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

A.17.1 Informatiebeveiligingscontinuïteit

Doelstelling: Informatiebeveiligingscontinuïteit moet worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie

A.17.1.1 Informatiebeveiligingscontinuïteit plannen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.	Y	Een organisatie behoort vast te stellen of de continuïteit van de informatiebeveiliging onder het beheerproces van de bedrijfscontinuïteit valt of onder het beheerproces van rampenherstel. Informatiebeveiligingseisen behoren te worden vastgesteld als de planning voor bedrijfscontinuïteit en rampenherstel wordt gemaakt. Bij afwezigheid van een formele planning voor bedrijfscontinuïteit en rampenherstel behoort het informatiebeveiligingsbeheer ervan uit te gaan dat informatiebeveiligingseisen in ongunstige situaties hetzelfde blijven als in normale uitvoeringsomstandigheden. In het andere geval kan een organisatie een bedrijfsimpactanalyse uitvoeren voor informatiebeveiligingsaspecten om de informatiebeveiligingseisen vast te stellen die van toepassing zijn op ongunstige situaties.	De volgende overwegingen zijn belangrijk in zorgomgevingen. Bedrijfscontinuïteitsmanagement, dat rampenherstel omvat, wordt steeds meer erkend als een vereiste voor gezondheidsorganisaties en er wordt een steeds hogere prioriteit aan toegekend. Met het oog op de strenge beschikbaarheidseisen in de zorg zou er veel moeten worden geïnvesteerd in regelingen voor veerkracht en redundantie, niet alleen met betrekking tot de technologie op zich, maar ook met betrekking tot de bredere opleiding van medewerkers in de zorg. Bedrijfscontinuïteitsplanning in de zorg is met name een uitdaging voor de informatiebeveiligingsprofessional, aangezien alle plannen op geschikte wijze behoren te worden geïntegreerd in de plannen van de organisatie voor het omgaan met stroomuitval, het implementeren van beheersing van infecties en het omgaan met andere klinische noodsituaties. Als er een beroep wordt gedaan op een van deze plannen, zal dit waarschijnlijk ook rechtstreeks leiden tot een beroep op het bedrijfscontinuïteitsmanagementplan, zij het alleen maar om extra ondersteuning te bieden naast de ondersteuning die normaal gesproken beschikbaar is. Recente incidenten, zoals de uitbraak van SARS, hebben echter aangetoond dat grote incidenten tot een personeelstekort kunnen leiden dat vervolgens het vermogen om plannen voor

			bedrijfscontinuïteitsmanagement op geslaagde wijze uit te voeren ernstig kan beperken. Zorginstellingen behoren te garanderen dat hun bedrijfscontinuïteitsmanagementplanning de planning van zorgcrisismanagement omvat. Levens van patiënten kunnen afhangen van de toegang tot patiëntgegevens en het is essentieel dat hiermee tijdens de planning rekening wordt gehouden. Catastrofes en crises waarbij er sprake is van overmacht waardoor IT-systemen in andere bedrijfstakken buiten werking gesteld worden, zijn juist de gebeurtenissen die kunnen leiden tot een crisis op het gebied van de volksgezondheid waarbij tijdige toegang tot gezondheidsinformatie cruciaal is. Gezondheidsorganisaties behoren ook te garanderen dat de plannen die ze ontwikkelen, regelmatig op 'programmatische' basis worden getoetst. De toetsen die in dat programma worden opgenomen, behoren op elkaar voort te bouwen, vanaf desktop-toetsen tot modulair toetsen tot een synthese van waarschijnlijke hersteltijden en ten slotte tot volledige oefeningen. Een dergelijk programma gaat derhalve met een laag risico gepaard en levert een echte verbetering op van het algemene bewustzijnsniveau van de gebruikerspopulatie. Ten slotte behoort de organisatie op de hoogte te blijven van de rol die gezondheidsinformatiesystemen spelen in de continuïteit van de zorg voor patiënten. Dergelijke organisaties behoren voorbereid te zijn indien/wanneer IT-systemen niet naar behoren werken.

A.17.1.2 Informatiebeveiligingscontinuïteit implementeren

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	Y	Een organisatie behoort ervoor te zorgen dat: a) er een adequate beheerstructuur is die is voorbereid op een verstorende gebeurtenis, deze verzacht en erop reageert met personeel dat beschikt over de nodige autoriteit, ervaring en competentie; b) personeel voor incidentrespons wordt aangesteld dat beschikt over de nodige verantwoordelijkheid, autoriteit en competentie om een incident te af te handelen en de informatiebeveiliging te handhaven; c) op basis van door de directie goedgekeurde doelstellingen voor informatiebeveiligingscontinuïteit, gedocumenteerde plannen, respons- en herstelprocedures worden ontwikkeld en goedgekeurd, waarin gedetailleerd wordt omschreven hoe de organisatie een verstorende gebeurtenis zal aanpakken en haar informatiebeveiliging op een vooraf vastgesteld niveau zal handhaven (zie 17.1.1).	Organisaties die persoonlijke gezondheidsinformatie verwerken, behoren processen, systemen en andere relevante uitrusting te identificeren die vitaal zijn voor de verlening van zorg. Om storingen in processen, systemen en relevante uitrusting die van vitaal belang zijn voor de zorgverlening op te vangen, behoren noodprocedures als noodzakelijk te worden beschouwd.

		In overeenstemming met de eisen voor informatiebeveiligingscontinuïteit behoort de organisatie het volgende vast te stellen, te documenteren, te implementeren en te onderhouden: a) beheersmaatregelen voor informatiebeveiliging binnen processen, procedures en ondersteunende systemen en instrumenten voor bedrijfscontinuïteit of rampenherstel; b) processen, procedures en implementatieveranderingen om bestaande beheersmaatregelen voor informatiebeveiliging tijdens een ongunstige situatie te handhaven; c) compenserende beheersmaatregelen voor beheersmaatregelen voor informatiebeveiliging die tijdens een ongunstige situatie niet kunnen worden gehandhaafd.	

A.17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	Y	Veranderingen betreffende de organisatie, procedures, processen of van technische aard, hetzij in een context van uitvoering, hetzij van continuïteit, kunnen leiden tot veranderingen in de eisen betreffende informatiebeveiligingscontinuïteit. In dergelijke gevallen behoort de continuïteit van processen, procedures en beheersmaatregelen voor informatiebeveiliging te worden beoordeeld tegen de achtergrond van deze veranderde eisen. Organisaties behoren de continuïteit van hun informatiebeveiligingsbeheer te verifiëren door: a) de functionaliteit van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te oefenen en te testen om te waarborgen dat ze consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit; b) de kennis en routine voor het uitvoeren van processen, procedures en beheersmaatregelen voor informatiebeveiligingscontinuïteit te oefenen en te testen om te waarborgen dat de prestaties consistent zijn met de doelstellingen van de informatiebeveiligingscontinuïteit; c) de deugdelijkheid en doeltreffendheid van maatregelen voor informatiebeveiligingscontinuïteit te beoordelen als informatiesystemen, informatiebeveiligingsprocessen, -procedures en -beheersmaatregelen, of de procedures en oplossingen van bedrijfscontinuïteitsbeheer of rampenherstelbeheer veranderen.	

A.17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen

A.17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	***N***	Organisaties behoren de bedrijfseisen voor de beschikbaarheid van informatiesystemen vast te stellen. Als de beschikbaarheid niet kan worden gegarandeerd door middel van de bestaande systeemarchitectuur, behoren redundante componenten of architecturen in overweging te worden genomen.	

		Indien van toepassing behoren redundante informatiesystemen te worden getest om te waarborgen dat de automatische omschakeling van de ene op de andere component bij storing werkt zoals voorzien.	

A.18 Naleving

A.18.1 Naleving van wettelijke en contractuele eisen

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen

A.18.1.1 Vaststellen van toepasselijke wetgeving en contractuele eisen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Y	Ook de specifieke beheersmaatregelen en individuele verantwoordelijkheden om aan deze eisen te voldoen behoren te worden gedefinieerd en gedocumenteerd. Managers behoren alle wetgeving die toepasselijk is op hun organisatie vast te stellen om te voldoen aan de eisen voor hun soort bedrijfsactiviteit. Indien de organisatie zakelijke activiteiten in andere landen verricht, behoren managers te letten op naleving in alle relevante landen.	Zorginstellingen behoren een auditprogramma voor naleving in te stellen dat ingaat op de volledige levenscyclus van de bedrijfsvoering, d.w.z. niet alleen van de processen waarmee knelpunten worden geïdentificeerd, maar ook van de processen die uitkomsten beoordelen, en over updates van het informatiebeveiligingsmanagementsysteem (ISMS) beslissen. De auditprogramma's van gezondheidsorganisaties behoren formeel te worden gestructureerd zodat ze alle elementen van deze internationale norm, alle risicogebieden en alle geïmplementeerde beheersmaatregelen binnen een cyclus van 12 maanden tot 18 maanden afdekken. In de sterk gereguleerde en gecontroleerde omgeving van veel zorginstellingen zou het ISMF (information security management forum) zichzelf als doel moeten stellen een gegradeerd kader voor controle op naleving vast te stellen, met als onderste laag een zelfaudit door degenen die de processen uitvoeren en de managers. Vervolgens behoren audits van het ISMS ten behoeve van het ISMF, interne audits, beoordelingen voor het borgen van beheersmaatregelen en externe audits dusdanig te worden gedefinieerd dat elke laag vertrouwen kan ontlenen aan alle lagen eronder.

A.18.1.2 Intellectuele-eigendomsrechten

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectueleeigendomsrechten en het gebruik van eigendomssoftwareproducten te	***N***	De volgende richtlijnen behoren in overweging te worden genomen om materiaal dat kan worden beschouwd als intellectuele eigendom te beschermen:	

waarborgen behoren passende procedures te worden geïmplementeerd.		a) een beleid ten aanzien van de naleving van intellectuele-eigendomsrechten publiceren dat het wettig gebruik van software en informatieproducten definieert; b) software alleen verkrijgen bij bekende bronnen met een goede reputatie, om te waarborgen dat het auteursrecht niet wordt geschonden; c) het bewustzijn in stand houden van het beleid voor de bescherming van intellectueleeigendomsrechten en bekendheid geven aan het voornemen om disciplinaire maatregelen te nemen tegen personeel dat deze rechten schendt; d) geschikte registers van bedrijfsmiddelen bijhouden, en alle bedrijfsmiddelen waarbij bescherming van intellectuele-eigendomsrechten vereist is identificeren; e) bewijs en bewijsmateriaal bijhouden van de eigendom van licenties, masterschijven, handleidingen enz. f) beheersmaatregelen implementeren om te bewerkstelligen dat een maximumaantal gebruikers dat eventueel door de licentie is toegestaan niet wordt overschreden; g) beoordelingen uitvoeren om te controleren dat alleen goedgekeurde software en in licentie gegeven producten zijn geïnstalleerd; h) een beleid vaststellen voor het handhaven van de juiste licentievoorwaarden; i) een beleid vaststellen voor het verwijderen van of aan anderen overdragen van software; j) voldoen aan voorwaarden voor software en informatie verkregen van openbare netwerken; k) niet dupliceren, naar een ander formaat converteren of een uittreksel maken van commerciële opnamen (film, audio), tenzij auteursrechtelijk toegestaan; l) geen boeken, artikelen, rapporten of andere documenten geheel of ten dele kopiëren, tenzij auteursrechtelijk toegestaan.	

A.18.1.3 Beschermen van registraties

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	***N***	Bij besluitvorming over bescherming van specifieke registraties van de organisatie behoort de classificatie daarvan, gebaseerd op het classificatieschema van de organisatie, in overweging te worden genomen. Registraties behoren te worden gecategoriseerd naar type, bijv. boekhoudkundige registraties, databaserecords, transactielogbestanden, auditlogbestanden en operationele procedures. Bij elk type behoort de bewaartermijn en toegestane soorten opslagmedia te worden vermeld, bijv. papier, microfiche, magnetische of optische opslag. Gerelateerde cryptografische sleutels en programma's die samenhangen met versleutelde archieven of digitale handtekeningen (zie hoofdstuk 10), behoren ook te worden bewaard om decodering van de registraties mogelijk te maken gedurende de bewaarperiode van de registraties. Er behoort rekening te worden gehouden met de mogelijkheid dat media die worden gebruikt om registraties te bewaren in kwaliteit achteruitgaan. Procedures voor bewaren en behandelen van deze media behoren te worden geïmplementeerd in overeenstemming met de aanbevelingen van de fabrikant. Als elektronische opslagmedia worden gekozen behoren procedures te worden vastgesteld om te waarborgen dat de gegevens tijdens de bewaarperiode toegankelijk blijven (leesbaarheid van zowel de media als van het gegevensformaat), om te voorkomen dat de informatie verloren gaat als gevolg van toekomstige technologische veranderingen.	

		Systemen voor gegevensopslag behoren zo te worden gekozen dat vereiste gegevens binnen een aanvaardbare tijdsspanne en in een aanvaardbaar formaat kunnen worden opgevraagd, afhankelijk van de eisen waaraan moet worden voldaan. Het systeem waarmee gegevens worden opgeslagen en behandeld, behoort de identificatie van registraties en hun bewaarperiode te waarborgen zoals gedefinieerd door, indien van toepassing, nationale of regionale wet- of regelgeving. Dit systeem behoort toe te staan dat registraties na afloop van die termijn op een passende manier worden vernietigd als de organisatie ze niet langer nodig heeft. Om te voldoen aan deze doelstellingen met betrekking tot het veiligstellen van registraties behoren binnen een organisatie de volgende stappen te worden genomen: a) er behoren richtlijnen te worden verstrekt voor het bewaren, opslaan, behandelen en verwijderen van registraties en informatie; b) er behoort een bewaarschema te worden opgesteld waarin registraties en de periode dat ze moeten worden bewaard, zijn vastgelegd; c) er behoort een inventarisoverzicht van bronnen van belangrijke informatie te worden bijgehouden.	

A.18.1.4 Privacy en bescherming van persoonsgegevens

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	Y	Organisaties behoren een beleid te ontwikkelen en te implementeren voor de privacy en bescherming van persoonsgegevens. Dit beleid behoort te worden gecommuniceerd aan alle personen die betrokken zijn bij het verwerken van persoonsgegevens. Naleving van dit beleid en van alle relevante wet- en regelgeving betreffende het beschermen van de privacy van personen en de bescherming van persoonsgegevens vereist een geschikte beheerstructuur en beheersing. Vaak kan dit het beste worden bereikt door een persoon te benoemen die hiervoor verantwoordelijk is, zoals een privacyfunctionaris, die richtlijnen behoort te geven aan managers, gebruikers en aanbieders van diensten over hun individuele verantwoordelijkheden en de specifieke procedures die behoren te worden gevolgd. Het toewijzen van verantwoordelijkheid voor het hanteren van persoonsgegevens en het waarborgen dat medewerkers zich bewust zijn van de privacyprincipes behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving. Er behoren passende technische en organisatorische maatregelen te worden geïmplementeerd om persoonsgegevens te beschermen.	Een voorbeeld van wet- of regelgeving waar geïnformeerde toestemming van patiënten wordt vereist, is de Aanbeveling van de Raad van Europa, R (97)5 betreffende de bescherming van medische gegevens, Raad van Europa, Straatsburg, 12 februari 1997: Alvorens een genetisch onderzoek wordt verricht behoort de betrokkene te worden geïnformeerd over het doel van het onderzoek en de mogelijkheid van onverwachte ontdekkingen. De aan een genetisch onderzoek onderworpen persoon behoort te worden ingelicht over onverwachte ontdekkingen indien aan de volgende voorwaarden is voldaan: a. dergelijke informatie is niet krachtens het interne recht verboden; b. de betrokkene heeft uitdrukkelijk om de informatie gevraagd; c. de informatie zal geen ernstige schade berokkenen: i. aan de gezondheid van de betrokkene; of ii. aan een bloedverwant van de betrokkene van vader- of moederszijde, iemand uit zijn directe omgeving, of iemand die

			direct verwant is aan dezelfde genetische stam als betrokkene. Een voorbeeld van een ethische beroepsrichtlijn die toestemming van de patiënt vereist, is de Verklaring van Helsinki van de Wereldgezondheidsorganisatie over medisch onderzoek op mensen. Verdere informatie over het managen van geïnformeerde toestemming in de zorg is te vinden in ISO/TS 17975.

A.18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	***N***	Voor de naleving van relevante overeenkomsten, wet- en regelgeving behoort met de volgende punten rekening te worden gehouden: a) beperkingen op de import of export van computerhardware en -software voor het uitvoeren van cryptografische functies; b) beperkingen op de import of export van computerhardware en -software die zo zijn ontworpen dat er cryptografische functies aan kunnen worden toegevoegd; c) beperkingen op de toepassing van codering; d) verplichte of discretionaire toegang voor nationale autoriteiten tot informatie die door hardware of software is versleuteld om in de vertrouwelijkheid van de inhoud te voorzien. Om naleving van de relevante wet- en regelgeving te waarborgen behoort juridisch advies te worden ingewonnen. Ook voordat versleutelde informatie of cryptografische beheersmaatregelen over grenzen van rechtsgebieden worden verstuurd, behoort juridisch advies te worden ingewonnen.	

A.18.2 Informatiebeveiligingsbeoordelingen

Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie

A.18.2.1 Onafhankelijke beoordeling van informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
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) behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	***N***	Deze onafhankelijke beoordeling behoort door de directie te worden geïnitieerd. Een dergelijke onafhankelijke beoordeling is nodig om te waarborgen dat de organisatie continu een geschikte, toereikende en doeltreffende aanpak van het beheer van informatiebeveiliging hanteert. Deze beoordeling behoort tevens het beoordelen van verbetermogelijkheden en de noodzaak om wijzigingen aan te brengen in de beveiligingsaanpak te omvatten, met inbegrip van het beleid en de beheersdoelstellingen. Een dergelijke beoordeling behoort te worden uitgevoerd door personen met een onafhankelijke positie ten opzichte van het te beoordelen gebied, bijv. door de interne auditor, een onafhankelijke manager of een externe organisatie die gespecialiseerd is in dergelijke beoordelingen. Personen die deze beoordelingen uitvoeren behoren te beschikken over passende vaardigheden en ervaring.	

		De resultaten van de onafhankelijke beoordeling behoren te worden vastgelegd en te worden gerapporteerd aan de directie die de beoordeling heeft geïnitieerd. Deze verslagen behoren te worden bewaard. Indien in de onafhankelijke beoordeling wordt vastgesteld dat de aanpak en de implementatie van het beheer van informatiebeveiliging van de organisatie ontoereikend zijn, bijv. gedocumenteerde doelstellingen en eisen zijn niet gehaald of niet in overeenstemming met de koers voor informatiebeveiliging zoals opgenomen in de beleidsregels voor informatiebeveiliging (zie 5.1.1), behoort de directie corrigerende maatregelen te overwegen.	

A.18.2.2 Naleving van beveiligingsbeleid en -normen

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
De directie behoort regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	Y	Managers behoren vast te stellen op welke manier wordt beoordeeld of is voldaan aan informatiebeveiligingseisen zoals gedefinieerd in beleidsregels, normen en andere toepasselijke regelgeving. Voor een doeltreffende regelmatige beoordeling behoort te worden overwogen om automatische meet- en rapportage-instrumenten in te zetten. Indien de beoordeling een geval van niet-naleving oplevert, behoren managers: a) de oorzaken van de niet-naleving vast te stellen; b) de noodzaak te evalueren tot het treffen van maatregelen om naleving te bewerkstelligen; c) passende corrigerende maatregelen te implementeren; d) de getroffen corrigerende maatregelen te beoordelen om de doeltreffendheid ervan te verifiëren en om gebreken of zwakke plekken te identificeren. Resultaten van door managers uitgevoerde beoordelingen en getroffen corrigerende maatregelen behoren te worden geregistreerd en deze verslagen behoren te worden bewaard. Managers behoren de resultaten te rapporteren aan de personen die onafhankelijke beoordelingen uitvoeren (zie 18.2.1) wanneer een onafhankelijke beoordeling plaatsvindt binnen hun verantwoordelijkheidsgebied.	

A.18.2.3 Beoordeling van technische naleving

Beheersmaatregel (ISO 27001)	SOA	Implementatierichtlijn	Zorgspecifieke implementatierichtlijn
Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Y	Technische naleving behoort bij voorkeur te worden beoordeeld met behulp van geautomatiseerde instrumenten die technische rapporten vervaardigen, die vervolgens door een technisch specialist worden geïnterpreteerd. Als alternatief kunnen handmatige beoordelingen (indien nodig ondersteund door passende software-instrumenten) door een ervaren systeemtechnicus worden uitgevoerd. Indien penetratietests of kwetsbaarheidsbeoordelingen worden toegepast is voorzichtigheid geboden omdat dergelijke activiteiten de beveiliging van het systeem kunnen compromitteren. Dergelijke tests behoren te worden gepland en gedocumenteerd en behoren herhaalbaar te zijn. Beoordeling van technische naleving behoort uitsluitend te worden uitgevoerd door competente, bevoegde personen of onder toezicht van dergelijke personen.	Er wordt speciaal gewezen op naleving in het kader van technische interoperabiliteit, aangezien grootschalige gezondheidsinformatiesystemen meestal uit een groot aantal onderling samenwerkende systemen bestaan.