A.5 Informatiebeveiligingsbeleid

A.5.1 Aansturing door de directie van de informatiebeveiliging

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

A.5.1.1 Beleidsregels voor informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Ten behoeve van informatiebeveiliging dienen een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen	Y	Elk ziekenhuis behoort over een geactualiseerd en gepubliceerd beleidsdocument voor informatieveiligheid te beschikken dat is goedgekeurd door de verantwoordelijke voor het dagelijkse bestuur (of gelijkwaardig). Alle elementen uit dit beleid, die een medewerker nodig heeft om zijn taken correct uit te voeren, moeten kenbaar gemaakt worden aan alle medewerkers, inclusief ingehuurde medewerkers en externe gebruikers die gebruik maken van de informatie beschikbaar op de systemen van het ziekenhuis.

A.5.1.2 Beoordeling van hetinformatiebeveiligingsbeleid

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Het beleid voor informatiebeveiliging dient met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	Y	Er dient regelmatig aan de verantwoordelijke voor het dagelijkse bestuur (of gelijkwaardig) gerapporteerd te worden over de stand van informatieveiligheid en bescherming van persoonsgegevens om de toepasbaarheid, volledigheid, adequaatheid en effectiviteit van informatieveiligheid en bescherming van persoonsgegevens te valideren. Vastgestelde afwijkingen, problemen of incidenten zullen tijdig opgevolgd worden met gepaste acties/sancties in lijn met de interne procedures van de organisatie. Ernstige incidenten of inbreuken in verband met persoonsgegevens worden altijd tijdig geëscaleerd naar de bevoegde instanties.

A.6.1.1Rollen en verantwoordelijkheden bij informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Alle verantwoordelijkheden bij informatiebeveiliging dienen worden gedefinieerd en toegewezen	Y	Elk ziekenhuis behoort te hebben: • een informatieveiligheidsdienst inrichten die wordt geleid door een informatieveiligheidsconsulent of DPO. • een informatieveiligheidsplan hebben dat door de verantwoordelijke voor het dagelijkse bestuur van het betrokken ziekenhuis (of gelijkwaardig) werd goedgekeurd. • over de nodige werkingskredieten beschikken die door de verantwoordelijke voor het dagelijkse bestuur van het betrokken ziekenhuis (of gelijkwaardig) werden goedgekeurd, om het informatieveiligheidsplan te kunnen uitvoeren en om de informatieveiligheidsdienst toe te laten de opgedragen taken uit te voeren. • de informatieveiligheidsconsulent of DPO betrekken bij de werkzaamheden van het ziekenhuis via het ter beschikking stellen van gegevens en via regelmatig overleg tussen de verschillende betrokken partijen.

A.6.1.2 Scheiding van taken

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting

Conflicterende taken en verantwoordelijkheden dienen te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.	Y	

A.6.1.3 Contact met overheidsinstanties

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Er dienen passende contacten met relevante overheidsinstanties worden onderhouden	N	Geen specifiek objectief gedefiniëerd. Dit onderdeel wordt centraal ondersteund

A.6.1.4 Contact met speciale belangengroepen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Er dienen passende contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties worden onderhouden	N	Geen specifiek objectief gedefiniëerd. Dit onderdeel wordt centraal ondersteund

A.6.1.5 Informatiebeveiliging in projectbeheer

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatiebeveiliging dient aan de orde komen in projectbeheer, ongeacht het soort project	Y	Elk ziekenhuis behoort te hebben: • bij elk proces en bij elk project een risico-beoordeling rond informatieveiligheid en bescherming van persoonsgegevens uitvoeren, valideren, communiceren en onderhouden • op het niveau van de verantwoordelijke van de verwerking alle risico-beoordelingen met een hoog residueel risico bespreken en waar nodig conform GDPR vóór de verwerking een raadpleging van de toezichthoudende autoriteit laten plaatsvinden.

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	Bijkomende toelichting
Beleid en ondersteunende beveiligingsmaatregelen dienen te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt, te beheren	Y	Elk ziekenhuisbehoort te hebben; • de gepaste maatregelen nemen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media enkel toegankelijk zijn voor geautoriseerde personen. • de gepaste maatregelen treffen, in functie van het toegangsmedium, voor de informatieveiligheid van de toegang van buiten het ziekenhuis tot de professionele, vertrouwelijke en gevoelige gegevens van de organisatie. • de voorwaarden opleggen, die gedetailleerd zijn in de beleidslijn 'mobiele toestellen', bij het gebruik van privé-toestellen voor beroepsdoeleinden. • de regels opleggen, die gedetailleerd zijn in de beleidslijn 'mobiele toestellen', bij het gebruik van de mobiele toestellen voor zowel beroepsdoeleinden als voor privé-doeleinden. • de eigen mobiele toestellen duidelijk identificeren, veilig configureren (met de nodige anti-malware software en met software die alle data op het toestel vanop afstand kunnen wissen) en de identificatie bijhouden in een centraal register.

		• de gebruikers regelmatig sensibiliseren omtrent de goede praktijken inzake gebruik en hun verantwoordelijkheden (zeker in verband met het connecteren tot publieke draadloze netwerken). • zich ertoe verbinden om de bescherming van persoonsgegevens van de gebruiker te respecteren.

A.6.2.2 Telewerken

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Beleid en ondersteunende beveiligingsmaatregelen dienen te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen	Y	Elk ziekenhuis behoort te hebben: • de gepaste maatregelen treffen, in functie van het toegangsmedium, voor de veiligheid van de toegang van buiten het ziekenhuis tot de professionele, vertrouwelijke en gevoelige gegevens van het ziekenhuis • duidelijk gedragsregels en een gepaste implementatie van toegang op afstand opzetten, valideren, communiceren en onderhouden, inclusief de uitwerking van welke systemen niet, en welke systemen wel vanop afstand of met gebruik van andere apparaten mogen worden geraadpleegd. • de gepaste maatregelen treffen om toestellen, vreemd aan het ziekenhuis, veilig toegang te geven aan de informatie indien daar een noodzaak toe is.

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	Bijkomende toelichting
Verificatie van de achtergrond van alle kandidaten voor een dienstverband dient te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de vastgestelde risico's	Y	

A.7.1.2 Arbeidsvoorwaarden

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
De contractuele overeenkomst met medewerkers en contractanten dient hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden	Y	Elk ziekenhuisbehoort voorafgaand aan het dienstverband: • De toekomstige medewerker te wijzen op het arbeidsreglement of de dienstregeling, waarin hun verantwoordelijkheden en die van het ziekenhuis ten aanzien van informatieveiligheid en bescherming van persoonsgegevens zijn vastgelegd. • Met de leverancier die medewerkers levert die met persoonsgegevens van het ziekenhuis in contact komen, contractuele afspraken maken waarbij de leverancier garandeert dat deze medewerkers de regels op vlak van informatieveiligheid en bescherming van persoonsgegevens die in het ziekenhuis gelden, zullen opvolgen.

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	Bijkomende toelichting
De directie dient van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie	Y	

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

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Alle medewerkers van de organisatie en, voor zover relevant, contractanten dienen een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie	Y	• De directie behoort van alle medewerkers te eisen dat ze informatieveiligheid en bescherming van persoonsgegevens toepassen overeenkomstig de informatieveiligheidsvoorschriften van het ziekenhuis • Alle medewerkers van het ziekenhuis moeten geschikte training en regelmatige bijscholing krijgen met betrekking tot minimale normen en procedures van de organisatie, voor zover relevant voor hun rol of functie • Elke organisatie moet minstens jaarlijks een sensibiliseringscampagne of informatiesessie met betrekking tot informatieveiligheid en bescherming van persoonsgegevens aanbieden

A.7.2.3 Disciplinaire procedure

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Er dient een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	Y	

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	Bijkomende toelichting
Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, dienen te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer worden gebracht	Y	

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	Bijkomende toelichting

Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, dienen te worden geïdentificeerd, en van deze bedrijfsmiddelen dient een inventaris te worden opgesteld en onderhouden	Y	Apparaten die de eigendom zijn of in beheer zijn van het ziekenhuis en waarop persoonsgegevens worden verwerkt dienen opgenomen te worden in een inventaris.

A.8.1.2 Eigendom van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, dienen een eigenaar hebben.	Y	

A.8.1.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, dienen regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd	Y	Het ziekenhuis dient een beleidslijn uit te werken waarbij wordt aangegeven dat de gebruiker steeds verantwoordelijk blijft voor bescherming van de informatie die in zijn bezit is, ongeacht de vorm waarin deze informatie wordt opgeslagen. De gebruiker moet dus zorgen voor een goede bescherming ervan door het naleven van de voorschriften die door het ziekenhuis worden opgesteld inclusief de vernietiging wanneer nodig en toegestaan.

A.8.1.4 Teruggeven van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Alle medewerkers en externe gebruikers dienen alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben, bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven	Y	Alle medewerkers behoren , na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, terug te geven en erop toe te zien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.

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	Bijkomende toelichting
Informatie dient te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging	Y	Elk ziekenhuis behoort een richtlijn te hebben betreffende een classificatieschema . De classificatie houdt rekening met het onderscheid tussen persoonsgegevens en niet-persoonsgegevens . De classificatie van gegevens dient in samenwerking met de DPO regelmatig gecontroleerd te worden

A.8.2.2 Informatie labelen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Om informatie te labelen dient een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Y	Elk ziekenhuis behoort de nodige maatregelen te treffen om de gebruikers van de informatie duidelijk te maken wat de classificatie van de informatie is. Dit kan gebeuren door het labelen van fysieke dragers van de informatie, door het melden van de classificatie in de toepassingen of middels de awareness sessies die door het ziekenhuis voorzien zijn.

A.8.2.3 Behandelen van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting

Procedures voor het behandelen van bedrijfsmiddelen diene te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Y	

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	Bijkomende toelichting
Voor het beheren van verwijderbare media dienen procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld	Y	Elk ziekenhuis behoort de nodige maatregelen te treffen om • te voorkomen dat informatie bewaard op fysieke media wordt vrijgegeven, gewijzigd, verwijderd of vernietigd zonder toelating. • fysieke media tijdens het transport te beschermen tegen niet geautoriseerde toegang. • fysieke media, inclusief mobiele media, veilig te vernietigen wanneer deze niet langer gebruikt worden

A.8.3.2 Verwijderen van media

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Media dienen op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Y	

A.8.3.3 Media fysiek overdragen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Media die informatie bevatten, dienen te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport	Y	

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	Bijkomende toelichting
Een beleid voor toegangsbeveiliging dient te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen	Y	

A.9.1.2 Toegang tot netwerken en netwerkdiensten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Gebruikers dienen alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn	Y	Elk ziekenhuis behoort de toegang tot de gegevens en informatiesystemen t beperken door middel van formele procedures voor het verlenen en intrekken van toegangsrechten tot informatiesystemen en -diensten en de rechten te beperken tot wat strikt noodzakelijk is voor de zorgverstrekker voor het uitvoeren van zijn/haar opdracht. Indien de elektronische verwerking van bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG) de verificatie vereist van relevante kenmerken of relaties van de gebruiker, worden deze kenmerken of relaties geraadpleegd

		• hetzij in de betrokken authentieke bronnen vastgelegd door het Beheerscomité van het eHealth-platform • hetzij in een gegevensbank van de organisatie of van een gezondheidsnetwerk waarvan de organisatie deel uitmaakt en die, waar nodig, gesynchroniseerd is met kwaliteitsvolle informatie uit de authentieke bronnen vastgelegd door het Beheerscomité van het eHealth-platform.

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	Bijkomende toelichting
Een formele registratie- en afmeldingsprocedure dient te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken	Y	

A.9.2.2 Gebruikers toegang verlenen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Een formele gebruikerstoegangsverleningsprocedure dient te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken	Y	

A.9.2.3 Beheren van speciale toegangsrechten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Het toewijzen en gebruik van speciale toegangsrechten dient te worden beperkt en beheerst	Y	Elk ziekenhuis behoort het toekennen van geprivilegieerde toegangsrechten aan informatiebeheerders te beperken tot wat strikt noodzakelijk is voor het beheer van de informatie en de systemen die hem zijn toevertrouwd. Het ziekenhuis zal de informatiebeheerder erop wijzen dat extra toegang ook extra verantwoordelijkheden met zich meebrengt. Het ziekenhuis controleert het gebruik van die geprivilegieerde toegangen.

A.9.2.4 Beheer van geheime authenticatie-informatie van gebruikers

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting

Het toewijzen van geheime authenticatie-informatie dient te worden beheerst via een formeel beheersproces	Y	De organisatie authentiseert de identiteit van de natuurlijke persoon die de bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG) verwerkt (de 'gebruiker').
		Deze authenticatie geschiedt
		• hetzij met een middel geïntegreerd in de Federal Authentication Service (FAS) van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform;
		• hetzij door een authenticatiesysteem eigen aan de organisatie
		  ○ mits een registratie van de identiteit geschiedt aan de hand van een eenmalig gebruik van een authenticatiemiddel geïntegreerd in de FAS van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform en
		  ○ mits het authenticatiesysteem eigen aan de aanbieder voldoet aan de voorwaarden voor een betrouwbaarheidsniveau 'substantieel' zoals gepreciseerd in de punten 2.1., 2.2.1. element 2, 2.2.3., 2.2.4., 2.3.1. (met

		uitzondering van element 1) en 2.4. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening en ○ mits het authenticatiemiddel gebruikt in het authenticatiesysteem eigen aan de aanbieder en het activeringsproces ervan voldoet aan de voorwaarden voor een betrouwbaarheidsniveau 'laag' in punt2.2.1. element 1 en punt 2.2.2. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening, en het zodanig is ontworpen dat het kan worden verondersteld slechts te worden gebruikt door de persoon aan wie het toebehoort.. Het minimumniveau in de FAS vastgesteld door het Beheerscomité van het eHealth-platform niveau is 400.

A.9.2.5 Beoordeling van toegangsrechten van gebruikers

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Eigenaren van bedrijfsmiddelen dienen toegangsrechten van gebruikers regelmatig te beoordelen	Y	

A.9.2.6 Toegangsrechten intrekken of aanpassen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten dienen bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen moeten ze worden aangepast	Y	

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	Bijkomende toelichting
Van gebruikers dient te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie	Y	Elk ziekenhuis zal ervoor zorgen dat de gebruiker voldoende maatregelen neemt om zijn authenticatieinformatie (gebruikersnaam en paswoord) te beschermen.

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	Bijkomende toelichting
Toegang tot informatie en systeemfuncties van toepassingen dient te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging	Y	

A.9.4.2 Beveiligde inlogprocedures

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Indien het beleid voor toegangsbeveiliging dit vereist, dient toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure	Y	De organisatie authentiseert de identiteit van de natuurlijke persoon die de bijzondere categorieën van persoonsgegevens bedoeld in artikel 9, 1. van de Algemene Verordening Gegevensbescherming (AVG) verwerkt (de 'gebruiker'). Deze authenticatie geschiedt

		• hetzij met een middel geïntegreerd in de Federal Authentication Service (FAS) van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform;
		• hetzij door een authenticatiesysteem eigen aan de organisatie
		  ○ mits een registratie van de identiteit geschiedt aan de hand van een eenmalig gebruik van een authenticatiemiddel geïntegreerd in de FAS van een niveau dat gelijk is aan of hoger is dan het niveau vastgesteld door het Beheerscomité van het eHealth-platform en
		  ○ mits het authenticatiesysteem eigen aan de aanbieder voldoet aan de voorwaarden voor een betrouwbaarheidsniveau 'substantieel' zoals gepreciseerd in de punten 2.1., 2.2.1. element 2, 2.2.3., 2.2.4., 2.3.1. (met uitzondering van element 1) en 2.4. van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 van de EIDAS-verordening en
		  ○ [3].
		Het minimumniveau in de FAS vastgesteld door het Beheerscomité van het eHealth-platform niveau is 400.

A.9.4.3 Systeem voor wachtwoordbeheer

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Systemen voor wachtwoordbeheer dienen interactief te zijn en sterke wachtwoorden waarborgen.	Y	Elk ziekenhuis zal ervoor zorgen dat de gebruiker voldoende maatregelen neemt om zijn authenticatieinformatie (gebruikersnaam en paswoord) te beschermen. Het systeem dat instaat voor de authenticatie dient afhankelijk van het risico en de technische mogelijkheden één of meerdere van volgende maatregelen te voorzien: • technische middelen voorzien voor multi-factor authenticatie • afdwingen van het gebruik van individuele gebruikers-ID's en wachtwoorden om verantwoording af te leggen; • gebruikers toestaan hun eigen wachtwoorden te selecteren en te wijzigen en een bevestigingsprocedure op te nemen in • handhaving van een keuze van kwaliteitswachtwoorden; • gebruikers dwingen hun wachtwoord te wijzigen bij de eerste aanmelding; • afdwingen van regelmatige wachtwoordwijzigingen en indien nodig; • een register bijhouden van eerder gebruikte wachtwoorden en hergebruik voorkomen; Voor het gebruik van wachtwoordsystemen dienen volgende maatregelen gerespecteerd te worden: • geen wachtwoorden op het scherm weergeven wanneer deze worden ingevoerd; • bewaar wachtwoordbestanden gescheiden van systeemgegevens van de applicatie; bewaar en verzend wachtwoorden in beveiligde vorm.

A.9.4.4 Speciale systeemhulpmiddelen gebruiken

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, dienen te worden beperkt en nauwkeurig worden gecontroleerd	N	

A.9.4.5 Toegangsbeveiliging op programmabroncode

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Toegang tot de programmabroncode dient te worden beperkt	N	

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	Bijkomende toelichting
Ter bescherming van informatie dient een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	N	Deze maatregelen zijn reeds opgenomen als mogelijke control voor het beschermen van informatie.

A.10.1.2 Sleutelbeheer

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels dient tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd	Y	Elk ziekenhuis voorziet in maatregelen voor het beschermen van encryptiesleutels. Deze maatregelen betreffen het beheer van certificaten aan de gebruikerszijde waarbij de sleutels dienen te worden beschermd tegen onbevoegd gebruik en ongewilde distributie.

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	Bijkomende toelichting
Beveiligingszones dienen te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.	Y	

A.11.1.2 Fysieke toegangsbeveiliging

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Beveiligde gebieden dienen te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt	Y	Elk ziekenhuis behoort toegangsbeveiligingen aan te brengen om ruimten te beschermen waar zich gevoelige of kritische informatie en informatica-voorzieningen bevinden zodat alleen bevoegd personeel toegang heeft.

A.11.1.3 Kantoren, ruimten en faciliteiten beveiligen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Voor kantoren, ruimten en faciliteiten dient fysieke beveiliging te worden ontworpen en toegepast.	Y	Zie A.11.1.2

A.11.1.4 Beschermen tegen bedreigingen van buitenaf

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Tegen natuurrampen, kwaadwillige aanvallen of ongelukken dient fysieke bescherming te worden ontworpen en toegepast	Y	Elk ziekenhuis behoort fysieke bescherming te realiseren tegen schade door brand, overstroming, inbraak en andere vormen van natuurlijke of menselijke calamiteiten alsook tegen schade als gevolg van een doelgerichte aanval.

A.11.1.5 Werken in beveiligde gebieden

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Voor het werken in beveiligde gebieden dienen procedures te worden ontwikkeld en toegepast.	N	Niet als apart punt opgenomen maar valt wel onder: Elk ziekenhuis behoort toegangsbeveiligingen aan te brengen om ruimten te beschermen waar zich gevoelige of kritische informatie en informatica-voorzieningen bevinden zodat alleen bevoegd personeel toegang heeft.

A.11.1.6 Laad- en loslocatie

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, dienen te worden beheerst, en zo mogelijk worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.	Y	Elk ziekenhuis ehoort toegangsbeveiligingen aan te brengen om ruimten te beschermen waar zich gevoelige of kritische informatie en informatica-voorzieningen bevinden zodat alleen bevoegd personeel toegang heeft.

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	Bijkomende toelichting
Apparatuur dient zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	Y	Apparatuur waarop persoonlijke informatie wordt verwerkt of die een kritische rol vervullen in de dienstverlening van het ziekenhuis moet zo worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.

A.11.2.2 Nutsvoorzieningen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Apparatuur dient te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen	Y	

A.11.2.3 Beveiliging van bekabeling

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, dienen te worden beschermd tegen interceptie, verstoring of schade	N	Reeds gecovered in netwerkbeveiliging.

A.11.2.4 Onderhoud van apparatuur

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Apparatuur dient correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen	N	Is reeds onderdeel van de beschikbaarheid

A.11.2.5 Verwijdering van bedrijfsmiddelen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting

Apparatuur, informatie en software dienen niet van de locatie worden meegenomen zonder voorafgaande goedkeuring	N	Deze maatregel is niet van toepassing voor ziekenhuizen waar o.a. artsen regelmatig informatie en toestellen zullen van de locatie meenemen. Bijkomende maatregelen om informatie te beschermen zitten reeds inclusief transport van informatie.

A.11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Bedrijfsmiddelen die zich buiten het terrein bevinden, dienen te worden beveiligd, waarbij rekening moet worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	N	Gecovered door 3rd party management voor wat betreft beheer van informatie off-site en telewerken.

A.11.2.7 Veilig verwijderen of hergebruiken van apparatuur

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Alle onderdelen van de apparatuur die opslagmedia bevatten, dienen 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	Elk ziekenhuis behoort de nodige maatregelen te treffen opdat alle gegevens op media gewist of ontoegankelijk gemaakt worden vóór verwijdering of hergebruik. Hierbij dient ook de nodige aandacht besteed te worden aan toestellen waarvan de primaire functie niet het stockeren van informatie is (zoals copiers) Dit geldt ook voor informatiedragers die niet de eigendom zijn van het hospitaal zijn en zal contractueel vastgelegd worden met de leverancier(s).

A.11.2.8 Onbeheerde gebruikersapparatuur

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Gebruikers dienen ervoor te zorgen dat onbeheerde apparatuur voldoende beschermd is	Y	Elk ziekenhuis behoort de nodige maatregelen te treffen om • te voorkomen dat informatie bewaard op fysieke media wordt vrijgegeven, gewijzigd, verwijderd of vernietigd zonder toelating. • fysieke media tijdens het transport te beschermen tegen niet geautoriseerde toegang.

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

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Er dient een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.	Y	Elk ziekenhuis behoort de nodige maatregelen te treffen om • te voorkomen dat informatie fysisch of digitaal ontoegankelijk is voor onbevoegden. (geen bruikbare informatie op het bureau of screensaver niet actief)

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	Bijkomende toelichting
Bedieningsprocedures dienen te worden gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.	Y	Elk ziekenhuis behoort minstens de documentatie te voorzien met betrekking tot backup, het opstarten en herstellen van systemen, beheer van loggegevens en monitorenvan activiteiten.

A.12.1.2 Wijzigingsbeheer

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, dienen te worden beheerst.	Y	Elk ziekenhuis behoort : • over procedures te beschikken voor het in productie stellen van nieuwe toepassingen en het aanpassen van bestaande toepassingen • te voorkomen dat één enkele persoon alleen de volledige controle zou verwerven over dit proces

A.12.1.3 Capaciteitsbeheer

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Het gebruik van middelen dient te worden gemonitord en afgestemd, en er moeten verwachtingen worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen	N	Gezien het spectrum van verschillende toestellen die gebruikt worden is dit eerder een operationeel punt meer dan een securitycontrol.

A.12.1.4 Scheiding van ontwikkel-, testen productieomgevingen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Ontwikkel-, test- en productieomgevingen dienen te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen	Y	Wanneer van toepassing behoort het ziekenhuis de gepaste maatregelen te treffen opdat • de productieomgeving gescheiden en verschillend is van de andere omgevingen zoals ontwikkeling, test, acceptatie, pre-productie, enz. • ervoor zorgen dat er geen testen of ontwikkelingen plaatsvinden in de productieomgeving. In bepaalde uitzonderlijke gevallen kan afgeweken worden van deze regel op voorwaarde dat gepaste maatregelen getroffen worden. • ervoor zorgen dat de informatie aanwezig op elk van de systemen conform alle regelgeving verwerkt wordt. Zo zullen de test, ontwikkeling en acceptatie-platformen van de nodige omkadering voorzien worden zodat de informatie conform GDPR en andere regelgeving verwerkt wordt.

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	Bijkomende toelichting
Ter bescherming tegen malware dienen beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers	Y	Elk ziekenhuis behoort over geactualiseerde systemen te beschikken ter bescherming (preventie, detectie en herstel) tegen malware. Daarnaast moeten geschikte procedures worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

A.12.3 Back-up

Doelstelling: Beschermen tegen het verlies van gegevens

A.12.3.1 Back-up van informatie

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Regelmatig dienen back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	Y	Om onherstelbaar verlies van gegevens te voorkomen, behoort elk ziekenhuis: • back-up-kopieën te nemen van informatie en programmatuur. • regelmatig de genomen back-ups te controleren op volledigheid en bruikbaarheid

		• De genomen backups beschermen tegen niet-geauthoriseerde toegang en vernietiging

A.12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

A.12.4.1 Gebeurtenissen registreren

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, dienen te worden gemaakt, bewaard en regelmatig worden beoordeeld	Y	Elk ziekenhuis behoort activiteiten van gebruikers met persoonsgegevens, uitzonderingen en gebeurtenissen vast te leggen in logbestanden. Deze logbestanden moeten gedurende een overeengekomen periode (gecommuniceerd naar de betrokken partijen)worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole rekening houdende met de regelgevingen mbt bescherming van persoonsgegevens. Logging biedt antwoord op minstens volgende functionaliteiten: • toelaten snel en eenvoudig te kunnen bepalen welke natuurlijke persoon, wanneer en op welke manier toegang heeft verkregen tot welke persoonsgegevens m.b.t. welke persoon; • de persoon die persoonsgegevens heeft verwerkt en de persoon waarover persoonsgegevens zijn verwerkt eenduidig kunnen identificeren; • de noodzakelijke tools ter beschikking hebben om toe te laten de loggegevens uit te baten door de geautoriseerde personen

A.12.4.2 Beschermen van informatie in logbestanden

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Logfaciliteiten en informatie in logbestanden dienen te worden beschermd tegen vervalsing en onbevoegde toegang	Y	

A.12.4.3 Logbestanden van beheerders en operators

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Activiteiten van systeembeheerders en -operators dienen te worden vastgelegd en de logbestanden dienen te worden beschermd en regelmatig worden beoordeeld	Y	

A.12.4.4 Kloksynchronisatie

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein dienen te worden gesynchroniseerd met één referentietijdbron	Y	Elk ziekenhuis behoort de klokken van zijn verschillende IT systemen met 1 referentietijdsbron synchroniseren. Deze synchronisatie is noodzakelijk om events op verschillende systemen met mekaar te kunnen in verband brengen en om reden van timestamping van bepaalde acties.

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	Bijkomende toelichting

Om het op operationele systemen installeren van software te beheersen dienen procedures te worden geïmplementeerd	Y	Elk ziekenhuis behoort : • over procedures te beschikken voor het in productie stellen van nieuwe toepassingen en het aanpassen van bestaande toepassingen

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	Bijkomende toelichting
Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt, dient tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden dient te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt, aan te pakken.	Y	Elk ziekenhuis behoort tijdig informatie te verzamelen over technische kwetsbaarheden van de gebruikte informatiesystemen of zich laten informeren door de leverancier. De mate waarin het ziekenhuis blootstaat aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten geschikte maatregelen worden genomen voor behandeling van daarmee samenhangende risico's.

A.12.6.2 Beperkingen voor het installeren van software

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Voor het door gebruikers installeren van software dienen regels te worden vastgesteld en geïmplementeerd	Y	Voor toestellen in eigen beheer geldt volgende: Elk ziekenhuis behoort : • over procedures te beschikken voor het in productie stellen van nieuwe toepassingen en het aanpassen van bestaande toepassingen

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	Bijkomende toelichting
Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, dienen zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	N	

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	Bijkomende toelichting
Netwerken dienen te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Y	Elk ziekenhuis behoort na te gaan of alle netwerken (inclusief draadloos) gepast beheerd en gecontroleerd worden zodanig dat ze beveiligd zijn tegen bedreigingen. Bovendien moet ze de beveiliging van de systemen en toepassingen die het netwerk gebruiken afdoende garanderen. Indien het netwerk niet de nodige garanties op bescherming kan bieden, dan dienen andere technieken zoals bv. encryptie overwogen te worden.

A.13.1.2 Beveiliging van netwerkdiensten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Beveiligingsmechanismen, dienstverleningsniveaus en beheerseisen voor alle netwerkdiensten dienen te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	Y	• Elk ziekenhuis behoort na te gaan of alle netwerken (inclusief draadloos) gepast beheerd en gecontroleerd worden zodanig dat ze beveiligd zijn tegen bedreigingen. Bovendien moet ze de beveiliging van de systemen en toepassingen die het netwerk gebruiken afdoende garanderen. • Elk ziekenhuis behoort de nodige technische maatregelen te implementeren om het hoogste niveau van beschikbaarheid voor haar diensten en externe verbindingen te waarborgen. Dit is nodig om een maximale toegankelijkheid van de beschikbaar gestelde en geraadpleegde gezondheidsgegevens te verzekeren

A.13.1.3 Scheiding in netwerken

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Groepen van informatiediensten, -gebruikers en -systemen dienen in netwerken te worden gescheiden.	N	Wordt afgedekt door minimalisatie van de toegangen naar de toepassingen en "Elk ziekenhuis behoort na te gaan of alle netwerken (inclusief draadloos) gepast beheerd en gecontroleerd worden zodanig dat ze beveiligd zijn tegen bedreigingen. Bovendien moet ze de beveiliging van de systemen en toepassingen die het netwerk gebruiken afdoende garanderen."

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	Bijkomende toelichting
Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, dienen formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	Y	Elk ziekenhuis behoort de nodige maatregelen te treffen om • fysieke media tijdens het transport te beschermen tegen niet geautoriseerde toegang • Het transport van informatie over netwerken dient afdoende bescherming te bieden.

A.13.2.2 Overeenkomsten over informatietransport

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Overeenkomsten dienen betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	N	Deze control spreekt over overeenkomsten maar dit dient een technische maatregel te zijn. Ook zijn er niet altijd overeenkomsten om gegevens te transporteren.

A.13.2.3 Elektronische berichten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatie die is opgenomen in elektronische berichten, dient passend beschermd te zijn.	Y	Informatiebeveiligingsoverwegingen voor elektronische berichten dienen het volgende te omvatten: • berichten beschermen tegen ongeautoriseerde toegang, wijziging of evenredige denial of service met het door de organisatie vastgestelde classificatieschema; • zorgen voor een correcte adressering en transport van het bericht;

A.13.2.4 Vertrouwelijkheids- of geheimhoudingsovereenkomst

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie	N	

weerspiegelen, dienen t worden vastgesteld, regelmatig worden beoordeeld en gedocumenteerd.		

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	Bijkomende toelichting
De eisen die verband houden met informatiebeveiliging dienen te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	Y	Elke organisatie behoort een efficiënte en constructieve communicatie op te zetten tussen de verschillende bij het project betrokken partijen (inclusief klanten en leveranciers), in het bijzonder met de informatieveiligheidsconsulent of DPO. Dit moet een adequaat niveau van informatieveiligheid en bescherming van persoonsgegevens garanderen gekend door iedereen en is noodzakelijk voor het toepassen van Data Protection by Design

A.14.1.2 Toepassingen op openbare netwerken beveiligen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, dient te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	N	Reeds opgenomen in netwerkbeveiliging

A.14.1.3 Transacties van toepassingen beschermen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatie die deel uitmaakt van transacties van toepassingen, dien te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.	N	

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	Bijkomende toelichting
Voor het ontwikkelen van software en systemen dienen regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie worden toegepast.	Y	Indien van toepassing moet de organisatie de 'secure project lifecycle' toepassen zoals beschreven in de beleidslijn 'Aankopen, ontwerpen, ontwikkelen en onderhouden van toepassingen'

A.14.2.2Procedures voor wijzigingsbeheer met betrekking tot systemen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling dienen te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	N	Reeds opgenomen in 12.5.1

A.14.2.3 Technische beoordeling van toepassingen na wijzigingen besturingsplatform

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Als besturingsplatforms zijn veranderd, dienen bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.	N	Hoewel het sterk aangeraden is om deze testen te laten doorgaan is de realiteit dat deze testen niet altijd kunnen plaatsvinden. De verantwoordelijke dient wel de nodige voorzieningen te treffen om de integriteit van de informatie en de verwerking ervan zo veel als mogelijk te testen voordat een kritische applicatie in dienst wordt gesteld na een update.

A.14.2.4 Beperkingen op wijzigingen aan softwarepakketten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Wijzigingen aan softwarepakketten dienen te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen dienen strikt te worden gecontroleerd.	N	Reeds opgenomen in 12.5.1

A.14.2.5 Principes voor engineering van beveiligde systemen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Principes voor de engineering van beveiligde systemen dienen te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	Y	Elke organisatie behoort een efficiënte en constructieve communicatie op te zetten tussen de verschillende bij het project betrokken partijen (inclusief klanten en leveranciers), in het bijzonder met de informatieveiligheidsconsulent of DPO. Dit moet een adequaat niveau van informatieveiligheid en bescherming van persoonsgegevens garanderen gekend door iedereen en is noodzakelijk voor het toepassen van Data Protection by Design

A.14.2.6 Beveiligde ontwikkelomgeving

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Organisaties dienen 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	Wanneer van toepassing behoort het ziekenhuis: • de gepaste maatregelen te treffen opdat de productieomgeving gescheiden en verschillend is van de andere omgevingen zoals ontwikkeling, test, acceptatie, pre-productie, enz. • ervoor te zorgen dat er geen testen of ontwikkelingen plaatsvinden in de productieomgeving. In bepaalde uitzonderlijke gevallen kan afgeweken worden van deze regel op voorwaarde dat gepaste maatregelen getroffen worden.

A.14.2.7 Uitbestede softwareontwikkeling

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Uitbestede systeemontwikkeling dient onder supervisie te staan van en te worden gemonitord door de organisatie.	Y	Zie 14.2.1. Bij het ter beschikking stellen van gegevens aan de ontwikkelpartij dienen de partijen een verwerkersovereenkomst af te sluiten.

A.14.2.8 Testen van systeembeveiliging

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Tijdens ontwikkelactiviteiten dient de beveiligingsfunctionaliteit te worden getest.	Y	Wanneer van toepassing behoort het ziekenhuis hierover te waken.

A.14.2.9 Systeemacceptatietests

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting

Voor nieuwe informatiesystemen, upgrades en nieuwe versies dienen programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Y	Elke organisatie behoort zich via de verantwoordelijke van de opvolging, de project leider, en bij de in productiestelling van het project er van te vergewissen dat de informatieveiligheidsvereisten en vereisten mbt bescherming van persoonsgegevens die vóór het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden

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	Bijkomende toelichting
Testgegevens dienen zorgvuldig te worden gekozen, beschermd en gecontroleerd.	Y	Elk ziekenhuis behoort ervoor te zorgen dat de informatie aanwezig op elk van de systemen conform alle regelgeving verwerkt wordt. Zo zullen de test, ontwikkeling en acceptatie-platformen van de nodige omkadering voorzien worden zodat de informatie conform GDPR en andere regelgeving verwerkt wordt. Dit betekent onder meer dat er geen reële persoonsgegevens in niet-productie-omgevingen mogen gebruikt worden.

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	Bijkomende toelichting
Met de leverancier dienen 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	In geval van uitbesteding aan derde partijen (inclusief "cloud computing" oplossingen) behoort elk ziekenhuis zich ervan te vergewissen dat: • de verplichtingen inzake de verwerking van persoonsgegevens contractueel zijn vastgelegd • de vereisten rond informatieveiligheid en bescherming van persoonsgegevens overeengekomen moeten worden met derde partijen en gedocumenteerd worden om risico's te reduceren met betrekking tot toegang van derde partijen tot informatiemiddelen. • de 'Richtlijnen rond veilig uitbesteding aan derde partijen' worden toegepast zoals beschreven in de beleidslijn 'Veilig uitbesteding aan derden'. • Een verwerkingsovereenkomst wordt gesloten met de leverancier volgens de bepalingen van GDPR. • Contractueel geregeld is wat er moet gebeuren met de gegevens als de samenwerking wordt gestopt

A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Alle relevante informatiebeveiligingseisen dienen 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	In geval van uitbesteding aan derde partijen (inclusief "cloud computing" oplossingen) behoort elk ziekenhuis zich ervan te vergewissen dat • alle relevante vereisten rond informatieveiligheid en bescherming van persoonsgegevens opgesteld en overeengekomen moeten worden met elk van die derde partijen die

		informatie van het ziekenhuis lezen, verwerken, stockeren, communiceren of ICT infrastructuurcomponenten aanleveren • overeenkomsten met derde partijen alle vereisten omvatten om risico's van informatieveiligheid en bescherming van persoonsgegevens te behandelen die geassocieerd zijn met ICT diensten • Een verwerkingsovereenkomst wordt gesloten met de leverancier volgens de bepalingen van GDPR

A.15.1.3 Toeleveringsketen van informatie- en communicatietechnologie

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Overeenkomsten met leveranciers dienen 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	Zie 15.1.2

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	Bijkomende toelichting
Organisaties dienen regelmatig de dienstverlening van leveranciers te monitoren, beoordelen en auditen.	Y	In geval van uitbesteding aan derde partijen (inclusief "cloud computing" oplossingen) behoort elk ziekenhuis zich ervan te vergewissen dat de dienstverlening van derde partijen regelmatig wordt gemonitord, geëvalueerd en geauditeerd.

A.15.2.2 Beheer van veranderingen in dienstverlening van leveranciers

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, dienen te worden beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.	Y	In geval van uitbesteding aan derde partijen (inclusief "cloud computing" oplossingen) behoort elk ziekenhuis zich ervan te vergewissen dat wijzigingen in de dienstverlening door derden worden beheerd, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatieveiligheid en bescherming van persoonsgegevens. Bij het beheren dient er rekening gehouden te worden met het kritieke karakter van de betrokken systemen en processen en met her-evaluatie van risico's.

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	Bijkomende toelichting

Directieverantwoordelijkheden en -procedures dienen te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Y	Elk ziekenhuis behoort procedures te hebben voor het vastleggen en beheren van incidenten over informatieveiligheid of bescherming van persoonsgegevens en de bijhorende verantwoordelijkheden. Deze procedures moeten bekend zijn bij alle medewerkers die betrokken zijn in het behandelen van informatieveiligheidsincidenten.

A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatiebeveiligingsgebeurtenissen dienen zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Y	Elke organisatie behoort : • Vast te leggen in het arbeidsreglement of dienstregeling dat elke medewerker (zowel vast of tijdelijk, intern of extern) verplicht is melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen. • Vast te leggen dat medewerkers gebeurtenissen en zwakheden over informatieveiligheid of bescherming van persoonsgegevens die verband houden met informatie en informatiesystemen aan de informatieveiligheidsdienst van het ziekenhuis moeten kenbaar maken, zodat het ziekenhuis tijdig en adequaat corrigerende maatregelen kan nemen. • Vast te leggen dat medewerkers incidenten over informatieveiligheid en bescherming van persoonsgegevens zo snel als mogelijk via de leidinggevende, de helpdesk, de informatieveiligheidsconsulent of functionaris van gegevensbescherming (DPO) rapporteren.

A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie, dient te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren.	Y	Het ziekenhuis ontwikkelt de policy die vastlegt dat medewerkers gebeurtenissen en zwakheden over informatieveiligheid of bescherming van persoonsgegevens die verband houden met informatie en informatiesystemen aan de informatieveiligheidsdienst van het ziekenhuis moeten kenbaar maken, zodat het ziekenhuis tijdig en adequaat corrigerende maatregelen kan nemen.

A.16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatiebeveiligingsgebeurtenissen dienen te worden beoordeeld en er moet worden geoordeeld of zij dienen te worden geclassificeerd als informatiebeveiligingsincidenten.	Y	Elk ziekenhuis behoort: • Elk incident over informatieveiligheid of bescherming van persoonsgegevens formeel te evalueren opdat procedures en controlemaatregelen verbeterd kunnen worden. De lessen die getrokken worden uit een incident dienen gecommuniceerd te worden naar de directie van het ziekenhuis voor validatie en goedkeuring van verdere acties. • Een proces te hebben voor de evaluatie van een incident dat onder meer bepaalt hoe beslist wordt om een incident al dan niet te melden aan de gegevensbeschermingsautoriteit en/of centrale meldingsdienst en hoe beslist wordt of de betrokkenen moeten geïnformeerd worden

A.16.1.5 Respons op informatiebeveiligingsincidenten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Op informatiebeveiligingsincidenten dient te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Y	Zie A.16.1.4

A.16.1.6 Lering uit informatiebeveiligingsincidenten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting

Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, dient te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	Y	Elke organisatie behoort elk incident over informatieveiligheid of bescherming van persoonsgegevens formeel te evalueren opdat procedures en controlemaatregelen verbeterd kunnen worden. De lessen die getrokken worden uit een incident dienen gecommuniceerd te worden naar de directie van het ziekenhuis voor validatie en goedkeuring van verdere acties

A.16.1.7 Verzamelen van bewijsmateriaal

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
De organisatie dient procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	Y	Het ziekenhuis behoort bij incidenten over informatieveiligheid of bescherming van persoonsgegevens het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften correct te verzamelen.

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	Bijkomende toelichting
De organisatie dient haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. Een crisis of een ramp, vast te stellen.	Y	Elk ziekenhuis behoort een eigen continuïteitsplan te hebben met minimaal aandacht aan: • Identificatie en documentatie van essentiële processen en bijhorende informatiesystemen van de organisatie; • Risico-beoordeling met invulling van kans, impact en huidige controlemaatregelen; • Kennis en competenties van medewerkers om essentiële processen en bijhorende informatiesystemen van het ziekenhuis draaiende te houden of weer op te starten; • Wie mag wanneer en hoe wordt het continuïteitsplan geactiveerd bij een ernstig incident of ramp; • Voor elke kritische toepassing beslissen hoe lang de toepassing maximaal mag onbeschikbaar zijn (return to operational) en of bij een incident dataverlies gedurende een korte vooraf vastgelegde periode aanvaardbaar is. Wat in die periode werd ingevoerd, zal opnieuw moeten ingevoerd worden. • Prioriteiten en volgorde van herstel; • Communicatie tijdens en na een ernstig incident of ramp; • Wie mag wanneer en hoe wordt het uitgevoerde continuïteitsplan formeel afgesloten na een ernstig incident of ramp.

A.17.1.2 Informatiebeveiligingscontinuïteit implementeren

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
De organisatie dient 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	Elk ziekenhuis behoort : • Voor alle kritieke processen en essentiële informatiesystemen een continuïteitsplan op te stellen, waarin activiteiten, maatregelen en belangrijke gegevens van de processen van het ziekenhuis worden beschreven, die tot doel hebben de onderbrekingstijd tot een aanvaardbaar niveau te beperken.

		• Informatieveiligheid en bescherming van persoonsgegevens als een integraal onderdeel van het continuïteitsbeheer uit te werken (zie beleidslijn 'Continuïteitsbeheer')

A.17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
De organisatie dient 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	Elk ziekenhuis behoort het continuïteitsplan regelmatig te testen en bij te sturen waar nodig. De resultaten van de testen behoren te worden geëvalueerd en gecommuniceerd naar de aangeduide verantwoordelijke van het ziekenhuis voor validatie en goedkeuring van verdere acties.

A.17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatieverwerkende faciliteiten bewerkstelligen

A.17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatieverwerkende faciliteiten dienen met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	N	Geen aparte norm. DRP zoals hier gevraagd kan worden ondergebracht in de volgende norm : *Voor alle kritieke processen en essentiële informatiesystemen een continuïteitsplan opstellen, waarin activiteiten, maatregelen en belangrijke gegevens van de processen van het ziekenhuis worden beschreven, die tot doel hebben de onderbrekingstijd tot een aanvaardbaar niveau te beperken*

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	Bijkomende toelichting
Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen dienen voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	Y	Elke organisatie behoort: • periodiek een conformiteitsonderzoek uit te voeren met betrekking tot de situatie rond informatieveiligheid en bescherming van persoonsgegevens zoals beschreven in de beleidslijnen. • schending te voorkomen van enige wetgeving, wettelijke, regelgevende, statutaire of contractuele verplichtingen gerelateerd aan informatieveiligheid en bescherming van persoonsgegevens. • zeker stellen dat informatieveiligheid en bescherming van persoonsgegevens geïmplementeerd en operationeel in overeenstemming is met de verwachtingen van de directie. • een formeel disciplinair proces hebben voor werknemers die inbreuk op de informatieveiligheid of bescherming van persoonsgegevens hebben gepleegd.

A.18.1.2 Intellectuele-eigendomsrechten

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectueleeigendomsrechten en het gebruik van	N	Niet van toepassing voor ziekenhuizen. (met uitzondering van licenties)

eigendomssoftwareproducten te waarborgen dienen passende procedures worden te geïmplementeerd.		

A.18.1.3 Beschermen van registraties

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Registraties dienen in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	N	Bescherming van records. Geen specifieke controle hierop nodig.

A.18.1.4 Privacy en bescherming van persoonsgegevens

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Privacy en bescherming van persoonsgegevensmoeten, voor zover van toepassing, dient te worden gewaarborgd in overeenstemming met relevante wet en regelgeving.	Y	Elke organisatie behoort : • regelmatig alle risico's in kaart te brengen in verband met de conformiteit met de Europese verordening. De geplande acties als gevolg van een hoog "residueel" risico op non-conformiteit dienen opgenomen te worden in het informatieveiligheidsplan van het ziekenhuis en desgevallend gerapporteerd naar de bevoegde autoriteiten conform GDPR. • In functie van de rol voor een specifieke (groep) verwerking (verwerker of verwerkings-verantwoordelijke), minimaal de volgende activiteiten uit te voeren: • de opname van de verwerking in het centraal register van de verwerkingsverantwoordelijke of van de verwerker; • een formele verantwoording voor het niet-realiseren van controlemaatregelen gericht op de naleving van de Europese verordening

A.18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Cryptografische beheersmaatregelen dienen te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	N	Domein is België. Kan bijkomend een punt worden wanneer gegevens in het buitenland worden gehost.

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	Bijkomende toelichting
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) dienen onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, te worden beoordeeld.	N	De naleving van de normen zal op regelmatig basis door de bevoegde overheid gecontroleerd worden waarbij volgende methodes kunnen overwogen worden: - Audit door externe bedrijven: een extern bedrijf zal aangesteld worden om de naleving van de normen na te gaan in de ziekenhuizen - Peer review: de ziekenhuizen stellen competente personen aan die kunnen deelnemen aan het uitvoeren van controle op de naleving van de normen binnen andere ziekenhuizen - Kwaliteitsaudits: de naleving van de minimale normen wordt nagegaan bij de kwaliteitsaudit van de ziekenhuizen (NIAS, JCI)

A.18.2.2 Naleving van beveiligingsbeleid en -normen

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting

De directie dient 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	Het ziekenhuis behoort voldoende kunnen aan te tonen dat er interne review heeft plaatsgevonden.

A.18.2.3 Beoordeling van technische naleving

Beheersmaatregel (ISO 27001)	SOA	Bijkomende toelichting
Informatiesystemen dienen regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Y	Zie A.18.2.2