Introductie

Dit toetsingskader is gebaseerd op de Gedragslijn 2.0. Het is opgebouwd uit drie tabbladen:
1. Gedragslijn 1.0 toetsingskader voor de aandachtsgebieden bewustwording, autorisaties, authenticatie en logging. Hierin zijn de wijzigingen verwerkt die zijn doorgevoerd in Gedragslijn 2.0.
2. Gedragslijn 2.0 toetsingskader voor het onderdeel ISMS
3. Gedragslijn 2.0 toetsingskader voor de aanvullende aandachtsgebieden, zoals cyber security en leveranciersmanagement.

Ieder tabblad bestaat uit de volgende structuur:

A - Het aandachtsgebied uit de Gedragslijn 2.0: De aandachtsgebieden komen overeen met de hoofdstukken van de Gedragslijn.

B - De referentie/paragraaf/normnummering van NEN 7510-1 (annex A).

C - Het onderwerp (of de beheersmaatregel) uit NEN 7510-1:2017 (annex A). De tekst is ongewijzigd overgenomen uit NEN 7510-1, inclusief de zorgspecifieke beheersmaatregel indien van toepassing.

D - De criteria uit de Gedragsljin 2.0 behorende bij de beheersmaatregel. De toetsingscriteria zijn ongewijzigd overgenomen uit de Gedragslijn 2.0. Voor tabblad 2 ISMS zijn geen criteria gedefinieerd in de Gedragslijn 2.0.

E - Testaanpak: Hulpmiddel voor het uitvoeren van een interne evaluatie/self-assessment. De testaanpak is een hulpmiddel ter aanvulling op de normbeschrijving, het vervangt de norm beschrijving derhalve niet. Instelling kan naar eigen inzicht afwijken van de testaanpak.

F - Resultaat opzet/bestaan. Hier geeft de instelling aan in hoeverre in opzet (gedocumenteerd) / bestaan (ingericht) wordt voldaan aan het criterium in termen van voldoet niet, deels of voldoet wel. Indien op alternatieve wijze wordt voldaan aan het criterium, kiest de instelling voor voldoet wel en licht dit toe in kolom F. bevindingen.

G - Bevindingen: Hier geeft de instelling de bevindingen weer, waaruit blijkt dat wel/deels/niet wordt voldaan aan het criterium. Aangevuld met toelichting, indien op alternatieve wijze het criterium wordt ingevuld (comply or explain).

H - Acties: hulpkolom voor de organisatie om de actie, actiehouder en deadline op te nemen, om de tekortkoming op te lossen.

I - Evidence: hulpkolom voor de organisatie om de verwijzing naar de evidence op te nemen, waaruit blijkt dat wel/niet wordt voldaan aan het criterium.

Gedragslijn 2.0 aandachtsgebied	Referentie NEN 7510-1:2017	Beheersmaatregel NEN 7510-1:2017 Annex A	Criteria Gedragslijn 2.0	Testaanpak (hulpmiddel voor self-assessment)	Resultaat opzet	Resultaat bestaan	Bevindingen	Acties	Evidence
Bewustwording medewerkers	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Beheersmaatregel (bron:. NEN 7510 deel 1 annex A) Alle medewerkers van de organisatie en, voor zover relevant, contractanten moeten een passende bewustzijnsopleiding en training krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van het beveiligingsbeleid en de procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken. Werknemers van de organisatie en, waar relevant, derde contractanten moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	a) Een bewustzijnsprogramma is opgesteld dat structureel geplande, periodiek geactualiseerde bewustwordingsactiviteiten bevat.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het bewustzijnsprogramma · Inspectie van de toegepaste bewustwordingsmiddelen (bijv. boekjes, nieuwsbrieven, presentaties en intranetberichten) · Stel vast hoe bij de instroom van nieuw personeel invulling wordt gegeven aan het bewustwordingsprogramma.					
			b) Het programma besteedt aandacht aan de basisprocedures inzake informatiebeveiliging (zoals het melden van informatiebeveiligingsincidenten/ datalekken) en basisbeheersmaatregelen (zoals wachtwoordbeveiliging, veilig delen van informatie, herkennen van verdachte e-mails, malwarecontroles, veilig gebruik van verwijderbare media en clean desk policy).	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het informatiebeveiligingsbeleid en aanverwante beleidstukken · Inspectie van het bewustzijnsprogramma					
			c) Het verantwoordelijk management ziet erop toe dat alle medewerkers (Personeel In Loondienst én Personeel Niet In Loondienst), onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken het bewustzijnsprogramma volgen bij indiensttreding en periodiek gedurende het dienstverband.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het HR indienst-, uitdienst- of ontslagproces van medewerker en personeel niet in loondienst v.w.b. het toepassen van bewustwording. · Inspectie van de resultaten van het bewustzijnsprogramma					
			d) Het bewustzijnsprogramma behoort periodiek 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.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van recent doorgevoerde wijzigingen aan het bewustzijnsprogramma					
			d) Het bewustzijnsprogramma behoort periodiek 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.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/ het bestaan vast van ingerichte maatregelen. · Inspectie van de resultaten van het bewustzijnsprogramma · Inspectie van door organisatie uitgevoerde analyses op de informatiebeveiligingsincidenten					
Autorisaties	A.9.1.1 Beleid voor toegangsbeveiliging	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs en informatiebeveiligingseisen. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie beperken tot situaties: a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt); b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben; c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen. Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. Het beleid van de organisatie met betrekking tot toegangscontrole behoort te worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol. Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, moet professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moet de taken die worden uitgevoerd door zorgverleners en de workflow van de taak in aanmerking nemen. De organisatie moet alle partijen identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen moeten contractuele afspraken over toegang en rechten worden gemaakt, alvorens cliëntgegevens uit te wisselen.	a) De organisatie heeft in het beleid voor toegangsbeveiliging passende regels vastgelegd voor de toegang tot en verwerking van informatie die aangeven hoe vigerende wet- en regelgeving en professionele en ethische richtlijnen met betrekking tot de toegang tot en verwerking van persoonlijke gezondheidsinformatie worden geïnterpreteerd en geïmplementeerd.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het beleid voor toegangsbeveiliging					
			b) De organisatie heeft op basis hiervan en op basis van de classificatie passende regels voor toegangsbeveiliging, rechten en beperkingen voor specifieke gebruikersrollen beschreven, waarbij de details en de striktheid van de beheersmaatregelen een afspiegeling zijn van de gerelateerde informatiebeveiligingsrisico's.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · inspectie van procedures voor autorisatiebeheer					
			c) Gebruikers en dienstverleners behoren een duidelijke instructie te ontvangen waarin is vastgelegd aan welke bedrijfseisen de toegangsbeveiligings-maatregelen moeten voldoen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het HR indienst proces (medewerkers, personeel niet in loondienst en inhuur) · Inspectie van de interne gedragscode					
			d) De organisatie heeft richtlijnen voor toegang middels noodprocedures.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van de noodprocedure · Stel in EPD vast dat noodprocedure functionaliteit inclusief logging is geactiveerd					
			e) Toegang tot persoonlijke gezondheidsinformatie is alleen toegestaan op basis van voorwaarden zoals vastgelegd in privacywetgeving, wet- en regelgeving omtrent het medisch beroepsgeheim en intern beleid. Voorbeelden van criteria (niet-limitatief) zijn: • Medewerkers hebben uitsluitend toegang tot persoonlijke gezondheidsinformatie indien zij een behandelrelatie hebben, dat wil zeggen rechtstreeks bij een behandeling betrokken zijn, of als toegang voor de beheersmatige afwikkeling van de behandeling noodzakelijk is. • De medewerker heeft uitsluitend toegang tot de persoonlijke gezondheidsinformatie die noodzakelijk is voor zijn/haar taak. Het gaat daarbij niet alleen om medische maar ook om administratieve ondersteuning en beheer van de instelling, voor zover de gegevens daarvoor noodzakelijk zijn (bijvoorbeeld het inschrijven van een patiënt, het inplannen van afspraken, het controleren van declaraties, het uitvoeren van kwaliteitsverbeteringsactiviteiten). • Toegang tot persoonlijke gezondheidsinformatie voor wetenschappelijk onderzoek kan alleen plaatsvinden indien daarvoor toestemming is verleend. De toestemming is niet vereist als het vragen daarvan in redelijkheid niet mogelijk is en de persoonlijke levenssfeer van de patiënt niet onevenredig wordt geschaad. Evenmin is toestemming vereist als het vragen daarvan in redelijkheid niet kan worden verlangd en redelijkerwijs wordt voorkomen dat de gegevens zijn te herleiden tot individuele personen. Gegevens mogen op grond van deze uitzonderingen alleen worden gebruikt indien het onderzoek een algemeen belang dient, het onderzoek niet zonder de betreffende gegevens kan worden uitgevoerd en de betrokken patiënt niet uitdrukkelijk bezwaar heeft gemaakt tegen de verstrekking van zijn gegevens (art. 7:458 lid 2 BW). Van de verstrekking van gegevens moet in het dossier een aantekening worden gemaakt.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het beleid voor toegangsbeveiliging · Inspectie van door organisatie uitgevoerde werkzaamheden (minimaal jaarlijks) dat functieprofielen in lijn zijn met het autorisatiebeleid. · Inspectie van het toestemmingsregister voor het gebruik van persoonlijke gezondheidsinformatie voor wetenschappelijk onderzoek					

Authenticatie	A.9.2.1 Registratie en afmelden van gebruikers	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Een formele registratie en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) De toegang tot gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers moeten garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratiegegevens moeten regelmatig worden beoordeeld om te garanderen dat deze volledig en juist zijn en dat toegang nog altijd vereist is.	a) De organisatie hanteert bij de registratie van verschillende soorten gebruikers procedures om toegangsrechten en bevoegdheden tot het netwerk, besturingssystemen, medische apparatuur, applicaties, informatie en externe gegevensuitwisseling toe te kennen of te wijzigen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het HR indienst proces, met specifiek aandacht voor het aanmaken van een gebruiker en het toekenningsproces van autorisaties					
			b) De organisatie hanteert bij de uitdiensttreding en/of het beëindigen van de opdracht procedures voor het intrekken van toegangsrechten en -bevoegdheden.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/ het bestaan vast van ingerichte maatregelen. · Inspectie van procedure voor intrekken / aanpassen logische toegangsrechten (bijvoorbeeld bij externen wordt bij aanvang de einde contractdatum als uitdienstdatum vastgelegd)					
			c) Als uitgangspunt voor de identificatie en authenticatie is hiervoor van belang dat medewerkers uitsluitend onder de eigen naam werken (authenticatie op naam). Indien gebruik wordt gemaakt van gedeelde accounts, dient de organisatie te borgen dat handelingen die met het account worden uitgevoerd wel herleidbaar zijn tot unieke personen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/ het bestaan vast van ingerichte maatregelen. · Inspectie van gebruikerslijsten - Inspectie van beleid / procedures over gebruik van gedeelde accounts indien van toepassing					
			d) Periodieke beoordeling van het overzicht van gebruikers met toegang, door of namens het management, vindt plaats om te garanderen dat dit volledig en juist is en dat toegang nog altijd vereist is.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat periodieke beoordeling van gebruikerslijsten door of namens het verantwoordelijk management plaatsvindt en bevindingen tijdig worden opgevolgd.					
			e) De taak van het identificeren en registreren van gebruikers van gezondheidsinformatiesystemen omvat de volgende punten: • het nauwkeurig vastleggen van de identiteit van een gebruiker (bijv. Jan Smit, geboren op 26 maart 1982, momenteel woonachtig op een specifiek adres); • 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); • het toewijzen van een ondubbelzinnige (naar een uniek persoon herleidbare) gebruikersidentificatiecode.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van gebruikerslijsten					
Autorisaties	A.9.2.2 Gebruikers toegang verlenen	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Een formele gebruikerstoegangsverleningsprocedure moet worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Geen	a) De organisatie heeft in een autorisatiematrix aangegeven welke soorten informatie voor welke functies van medewerkers voor de uitvoering van hun werk noodzakelijk zijn.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat een autorisatiematrix is opgesteld en is geaccordeerd door het management					
			b) De organisatie hanteert een systematiek van functies met daaraan rollen gekoppeld en gebruikt de combinatie van functie + rol(len) voor het toekennen van algemene toegangsrechten en systeembevoegdheden.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat rollen in het EPD worden gebruikt voor toekenning van rechten.					
			c) De organisatie kent de individuele medewerker/gebruiker op basis van functie + rol + plaats + positie in de organisatie, specifieke rollen en (systeem-) bevoegdheden (autorisaties) toe.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van gebruikerstoegangsverleningsprocedure					
			d) Periodieke beoordeling van de toegangsrechten (autorisaties) aan de hand van de autorisatiematrix vindt plaats om te garanderen dat toegangsrechten voldoende beperkt zijn en dat toegang nog altijd vereist is.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat periodieke beoordeling van de toegangsrechten door of namens het verantwoordelijk management plaatsvindt.					
Autorisaties	A.9.2.3 Beheren van speciale toegangsrechten	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Het toewijzen en gebruik van speciale toegangsrechten moet worden beperkt en beheerst. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Geen	a) De organisatie heeft procedures om ten behoeve van het functioneel en technisch beheer van systemen aan beheerders speciale bevoegdheden toe te kennen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het beleid c.q. procedures voor toekennen speciale bevoegdheden aan IT-beheerders en gebruikers met beheerrechten.					
			b) De betrokken medewerkers zijn bevoegd en bekwaam voor de uitvoering van de specifieke taken.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van IT-opleidingsplannen					
			c) Uitvoering van de specifieke taken en het gebruik van de speciale bevoegdheden worden gelogd.	· Interview de verantwoordelijke functionarissen · Inspectie van de wijze waarop organisatie de inrichting van logging op speciale bevoegdheden heeft beoordeeld					
			d) Het verantwoordelijk management ziet toe op de naleving en blokkeert de bevoegdheden (tijdelijk) wanneer gebruik niet (langer) noodzakelijk is.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat de periodieke beoordeling van de toegekende speciale bevoegdheden aan medewerkers door of namens het verantwoordelijk management plaatsvindt.					
Autorisaties	A.9.2.5 Beoordeling van toegangsrechten van gebruikers	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Geen	a) De organisatie beoordeelt minimaal jaarlijks voor reguliere gebruikers en minimaal halfjaarlijks voor gebruikers met beheerbevoegdheden dat toegangsrechten en bevoegdheden van de medewerkers actueel en conform het beleid en de autorisatiematrix zijn toegekend. Indien de organisatie op basis van een uitgevoerde risicoanalyse besluit om deze termijn (voor bepaalde omgevingen) ruimer te stellen, wordt dit gedocumenteerd en door het verantwoordelijk management bekrachtigd.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat de periodieke beoordeling van de toegekende speciale bevoegdheden aan medewerkers door of namens het verantwoordelijk management plaatsvindt. Zie ook 9.2.1.d, 9.2.2.e en 9.2.3.d.					

Autorisaties	A.9.2.6 Toegangsrechten intrekken of aanpassen	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd en bij wijzigingen moeten ze worden aangepast. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Alle organisaties die persoonlijke gezondheidsinformatie verwerken, moeten voor elke vertrekkende afdelingsmedewerker of tijdelijke medewerker, derde contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie beëindigen.	a) De organisatie heeft een procedure met betrekking tot het intrekken/aanpassen van logische toegangsrechten.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van procedure voor intrekken / aanpassen logische toegangsrechten. · Stel vast dat in de procedure is geborgd dat toegangsrechten van medewerkers tijdig worden ingetrokken bij uitdiensttreding of einde inhuurcontract.						
			b) De organisatie wijzigt de logische toegangsrechten van medewerkers bij elke wisseling van functie en/of werkplek van de medewerker binnen 24 uur. Indien de organisatie op basis van een risicoanalyse besluit om deze termijn (voor bepaalde omgevingen) ruimer te stellen, wordt dit gedocumenteerd en door het verantwoordelijk management bekrachtigd.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast op welke wijze de organisatie borgt (bij voorkeur middels tooling of een application control) dat toegangsrechten van medewerkers tijdig worden ingetrokken bij functiewijziging.						
			c) De organisatie beëindigt de logische toegangsrechten van medewerkers bij einde dienstverband of einde opdracht binnen 24 uur. Indien de organisatie op basis van een uitgevoerde risicoanalyse besluit om deze termijn (voor bepaalde omgevingen) ruimer te stellen, wordt dit gedocumenteerd en door het verantwoordelijk management bekrachtigd.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast op welke wijze de organisatie borgt (bij voorkeur middels tooling of een application control) dat toegangsrechten van medewerkers tijdig worden ingetrokken bij uitdiensttreding of einde inhuurcontract.						
			d) De organisatie heeft een procedure ingericht om toegangsrechten direct in te trekken, ingeval het verantwoordelijk management de beëindiging van het dienstverband heeft geïnitieerd ter voorkoming van het risico dat misnoegde medewerkers opzettelijk informatie corrumperen, systemen saboteren of zich onrechtmatig informatie toe-eigenen waar ze geen recht meer op hebben.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van procedure intrekken toegangsrechten bij ontslag.						
Authenticatie	A.9.4.1 Beperking toegang tot informatie	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij tenminste twee factoren betrokken worden. De toegang tot functies van informatie en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie moet gelsoleerd (en gescheiden) worden van de toegang tot de informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.	a) Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen. Dit moet worden gedaan door middel van multi-factor authenticatie (verder MFA) door middel van minimaal twee verschillende factoren.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat in het authenticatie beleid de uitgangspunten en inrichtingsprincipes van MFA zijn beschreven. · Inspectie van middelen voor MFA en de instellingen van deze middelen.						
			b) De organisatie hanteert voor externe toegang tot systemen die persoonlijke gezondheidsinformatie bevatten adequaat beveiligde verbindingen (gebruikmakend van versleutelde verbindingen), waarbij MFA door middel van minimaal twee verschillende factoren is ingericht.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast voor 1 aselect gekozen gebruiker dat inloggen in systemen met persoonlijke gezondheidsinformatie alleen toegestaan is door middel van MFA waarbij minimaal 2 factoren zijn betrokken. · Stel vast voor 1 aselect gekozen gebruiker dat inloggen vanuit externe locaties adequaat beveiligde verbinding plaatsvindt.						
			c) De organisatie hanteert op het interne netwerk een MFA door middel van minimaal twee verschillende factoren, tenzij er een gegronde reden (stand der techniek, patiëntveiligheid, infectiepreventie, etc.) is om hiervan af te wijken en het verantwoordelijk management door middel van risicoanalyse afwijkend beleid en passende alternatieve maatregelen voor toegang tot persoonlijke gezondheidsinformatie heeft vastgesteld: • Voor situaties waar intern gebruik van MFA andere thema's raakt (o.a. patiëntveiligheid, infectiepreventie, werkbaarheid) zoals op de SEH of OK, voert de organisatie een risicoanalyse uit volgens een algemeen geaccepteerde methode zoals Prospectieve Risico Inventarisatie (verder PRI). • De organisatie richt op basis van de uitkomsten van de risicoanalyse met alternatieve maatregelen een beheersingsniveau in dat gelijkwaardig is aan het niveau dat bereikt zou worden met MFA. Dit wordt vastgelegd en door het verantwoordelijk management bekrachtigd. • Indien het door zwaarwegende redenen vanuit eerdergenoemde andere thema's niet mogelijk is om een aan MFA gelijkwaardig niveau te realiseren, bijvoorbeeld vanuit patiëntveiligheid, worden op basis van de uitgevoerde risicoanalyse passende maatregelen getroffen en het besluit hiertoe gedocumenteerd en door het verantwoordelijk management bekrachtigd. • Daar waar zorginstellingen de mogelijkheid bieden om een gebruikerssessie 'mee te nemen' (gracing) naar een andere werkplek door middel van het aanbieden van een strikt individuele/persoonlijke token (bijvoorbeeld een medewerkerspas), wordt één van de volgende maatregelen geïmplementeerd. Randvoorwaardelijk hierbij is dat het beleid van de instelling erin voorziet dat een medewerker de token altijd bij zich draagt en bij vermissing van de token de medewerker hier onmiddellijk melding van maakt, waarna de token direct (tijdelijk) wordt geblokkeerd. 1) De medewerker neemt de sessie mee naar een andere werkplek, waar dan weer opnieuw door middel van MFA wordt ingelogd. Hiermee wordt MFA bij iedere inlog gerealiseerd. 2) De medewerker neemt de sessie mee door middel van toegang met één factor, zoals het aanbieden van een token. De zorginstelling hanteert een maximale termijn tussen het moment dat de laatste gebruikersactiviteit plaatsvond en het moment dat de token opnieuw is aangeboden op een (ander) werkstation van maximaal vier uur. Na het verstrijken van deze termijn, is opnieuw authenticatie met MFA vereist. 3) De medewerker neemt de sessie mee door het aanbieden van een token. De zorginstelling hanteert een maximale termijn vanaf het moment van aanloggen van maximaal vier uur. Na het verstrijken van deze termijn, is opnieuw authenticatie met MFA vereist.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel vast dat MFA gebruik maakt van minimaal twee factoren, die verschillen in de eigenschappen kennis, bezit en overerving. · Stel vast dat voor situaties is afgeweken ivm patiëntveiligheid een PRI is uitgevoerd. · Stel vast dat aanvullende maatregelen zijn getroffen, zodat een gelijkwaardig niveau wordt bereikt als middels MFA, bijvoorbeeld door de inzet van fysieke beveiligingsmaatregelen; · Stel vast dat de risicoanalyse en maatregelen zijn gedocumenteerd en bekrachtigd door management. · Inspectie van beleid / procedure voor het persoonsgebonden bezit van de token en het melden en blokkeren van de token bij vermissing · Stel vast door middel van inspectie van systeeminstellingen dat een sessie alleen kan worden meegenomen als is voldaan aan 1 van de 3 maatregelen. · Stel vast door middel van 1 aselect gekozen gebruiker dat de gebruikerssessie alleen kan worden meegenomen als is voldaan aan 1 van de 3 maatregelen.						
Authenticatie	A.9.4.3 Systeem voor wachtwoordbeheer	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Geen	a) De organisatie zorgt dat vereiste wachtwoordconventies door systeeminstellingen worden ondersteund en afgedwongen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van de wachtwoordpolicy's · Inspectie van wachtwoordinstellingen aan de hand van het intern wachtwoordbeleid of best practice instellingen.						
Logging en controle van logging	A.12.4.1 Gebeurtenissen registreren	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, bewaard en regelmatig worden beoordeeld. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Geen	a) De organisatie maakt het door middel van logging mogelijk achteraf onweerlegbaar vast te stellen welke gebeurtenissen hebben plaatsgevonden op een digitaal patiëntdossier.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het logging beleid of de logging procedure						
			b) De bewaartermijn voor logging is minimaal vijf (5) jaar (60 maanden) of zo lang als het dossier wordt bewaard.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van de logfiles om vast te stellen dat logbestanden minimaal 5 jaar worden bewaard.						

			c) Alle gebeurtenissen waarbij acties plaatsvinden die betrekking hebben op een patiëntdossier, moeten worden gelogd. Hiertoe behoren: • dossier aanmaken (een 'nieuwe map' die deel zal gaan uitmaken van een patiëntdossier); • identificator, bijvoorbeeld een dossiernummer, toekennen; • gegevens invoeren; • gegevens toevoegen; • gegevens verwijderen, al dan niet op verzoek van de cliënt; • gegevens lezen; • gegevens kopiëren of afdrukken; • dossiers samenvoegen of splitsen; • overdragen van gegevens vanuit of naar een ander systeem of informatiedomein, met inbegrip van kopiëren op draagbare media; • zoekacties.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het logging beleid of de logging procedure					
			d) Alle gebeurtenissen die niet vallen onder de normale procedures voor toegang tot gegevens (van het patiëntdossier) moeten worden gelogd, zoals: • toepassen van een noodprocedure; • directe toegang tot bestanden buiten de reguliere toegangsbeveiliging om, bijvoorbeeld voor het onderzoeken of herstellen van technische problemen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het logging beleid of de logging procedure · Stel (in samenhang met A.9.1.1.e) voor 1 testpatiënt in de logging vast dat de gebeurtenis wordt gelogd als de noodprocedure voor deze patient wordt geactiveerd.					
			e) In het algemeen moet de logging het mogelijk maken achteraf onweerlegbaar vast te stellen welke gebeurtenissen hebben plaatsgevonden op een patiëntdossier. Daartoe moeten alle systemen die gegevens bevatten die deel uitmaken van een patiëntdossier, daarover ten minste bijhouden: • welke gebeurtenis heeft plaatsgevonden; • datum en tijdstip van de gebeurtenis; • welke cliënt het betrof; • wie de gebruiker was.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het logging beleid of de logging procedure · Stel door middel van inspectie van uitgevoerde controles op logging vast dat logging risicogericht is beoordeeld op de in de norm genoemde elementen.					
			f) Zorginstellingen controleren de logging bij voorkeur door middel van geautomatiseerde of integrale controle. De controle van logging kan ook plaatsvinden door middel van deelwaarneming en steekproef. De controle van logging richt zich minimaal op de logresultaten van de noodprocedure ('breaking the glass'-procedure) en reguliere toegang tot patiëntdossiers. • Controle van de logresultaten van de noodprocedure is een procesgerichte controle en kan door middel van deelwaarnemingen worden gecontroleerd. Het aantal te controleren gebeurtenissen dient op jaarbasis minimaal zestig (60) te zijn. Het aantal van zestig (60) deelwaarnemingen is toegelicht in bijlage 3. • Controle van de logging van toegang tot patiëntdossiers is een gegevensgerichte controle en kan door middel van een statistische steekproef worden uitgevoerd. In geval van een homogene massa en een 0-fouten hypothese is de steekproefomvang in dit geval minimaal zestig (60) patiëntdossiers op jaarbasis. De steekproefomvang van 60 is toegelicht in bijlage 3. • De controles worden bij voorkeur evenredig over het jaar verspreid en in een maandelijkse frequentie uitgevoerd, zodat resultaten tijdig aan de betrokken medewerkers worden teruggekoppeld. • De zorginstelling kan er op basis van een risicoanalyse voor kiezen om een ander aantal controles uit te voeren. De keuze hiervoor wordt door het verantwoordelijk management gemaakt en wordt schriftelijk vastgelegd. • De uitgevoerde controles op de logging en het vervolg dat hieraan wordt gegeven, worden schriftelijk vastgelegd.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Inspectie van het logging beleid of de logging procedure · Inspectie van door organisatie uitgevoerde controles op de logging van toegang tot persoonlijke gezondheidsinformatie. · Stel door middel van inspectie van uitgevoerde controles op logging vast dat logging risicogericht is beoordeeld. · Stel door middel van inspectie van uitgevoerde controles op logging vast dat uitgevoerde controles en het vervolg dat hieraan wordt gegeven zijn gedocumenteerd.					
			g) In alle gevallen waarbij een onregelmatigheid wordt geconstateerd, zal de organisatie op korte termijn nader onderzoek doen. In die gevallen waar ongeautoriseerde toegang tot het digitaal patiëntdossier heeft plaatsgevonden, zal de organisatie, tenzij er zwaarwegende redenen zijn om dat niet te doen, betrokkene(n) informeren en gepaste actie richting de medewerker ondernemen conform het sanctiebeleid van de organisatie en hieraan opvolging geven conform de datalekkenprocedure.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel door middel van inspectie van uitgevoerde controles op logging vast dat onregelmatigheden adequaat zijn opgevolgd.					
			h) Het proces van beoordelingen van de logging wordt periodiek (ten minste eenmaal per jaar) afgestemd met het verantwoordelijk management. Zij beoordelen of de controles effectief zijn als onderdeel van de governance. Wanneer uit de beoordeling van de logging structurele tekortkomingen in de toegangsverlening van patiëntdossiers naar voren zijn gekomen, neemt de zorginstelling hierop passende maatregelen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel door middel van inspectie van uitgevoerde controles op logging vast dat het verantwoordelijk management periodiek de effectiviteit van het proces van beoordelen van logging beoordeelt.					
Logging en controle van logging	A.12.4.2 Beschermen van informatie in logbestanden	Beheersmaatregel (bron: NEN 7510 deel 1 annex A) Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang. Zorgspecifieke beheersmaatregel (bron: NEN 7510 deel 1 annex A) Auditverslagen moeten beveiligd zijn en mogen niet gemanipuleerd kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten moet worden beveiligd om misbruik of compromittering te voorkomen.	a) De organisatie heeft maatregelen getroffen om de toegang tot de logging te beperken tot bevoegde personen om wijzigingen of onbedoelde overschrijving van logging te voorkomen.	· Stel door middel van interview met de door de organisatie aangewezen verantwoordelijk functionaris(sen), de opzet/het bestaan vast van ingerichte maatregelen. · Stel door middel van inspectie van logging beleid of de logging procedure vast dat maatregelen zijn getroffen om de toegang tot de logging te beperken tot bevoegde personen.					

Gedragslijn 2.0 aandachtsgebied	Referentie NEN 7510-1:2017	Beheersmaatregel NEN 7510-1:2017	Testaanpak (hulpmiddel voor self-assessment)	Resultaat opzet	Resultaat bestaan	Bevindingen	Acties	Evidence
4 Context van de organisatie	4.1 Inzicht verkrijgen in de organisatie en haar context	De organisatie moet externe en interne onderwerpen vaststellen die relevant zijn voor haar doelstelling en die haar vermogen beïnvloeden om het (de) beoogde resulta(a)t(en) van haar managementsysteem voor informatiebeveiliging te behalen.	- Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. - Inspectie van beleid/strategie dat doelstellingen zijn geformuleerd met betrekking tot informatiebeveiliging. - Ga na of organisatie interne en externe onderwerpen heeft vastgesteld en gedocumenteerd, die relevant zijn voor het realiseren van de doelstellingen mbt informatiebeveiliging. - Ga na dat wettelijke vereisten hierin zijn meegenomen					
	4.2 Inzicht verkrijgen in de behoeften en verwachtingen van belanghebbenden	De organisatie moet vaststellen: a) welke belanghebbenden relevant zijn voor het managementsysteem voor informatiebeveiliging, en b) welke eisen van deze belanghebbenden relevant zijn voor informatiebeveiliging.	- Inspectie van het overzicht van belanghebbenden en hun eisen t.a.v. informatiebeveiliging. - Ga na hoe de organisatie wettelijke vereisten hierin heeft meegenomen - Interview een (select aantal) belanghebbende(n) en valideer of eisen zijn meegenomen.					
	4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen	De organisatie moet de grenzen en toepasselijkheid van het managementsysteem voor informatiebeveiliging bepalen om het toepassingsgebied ervan vast te stellen. Bij het vaststellen van dit toepassingsgebied moet de organisatie: a) de in 4.1 genoemde externe en interne onderwerpen overwegen, evenals; b) de in 4.2 genoemde eisen, en c) raakvlakken en afhankelijkheden tussen de activiteiten die door de organisatie en de activiteiten die door andere organisaties worden verricht. Het toepassingsgebied moet als gedocumenteerde informatie beschikbaar zijn.	- Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. - Inspectie van de documentatie van het toepassingsgebied. - Ga na of in de beschijving van het toepassingsgebied de interne en externe factoren, de eisen van belanghebbenden en de raakvlakken/afhankelijkheden met andere organisaties zijn meegenomen. - Ga na in hoeverre het toepassingsgebied van het ISMS volledig is, d.w.z. het bevat alle verwerkingen van de persoonsgegevens van patiënten, alsook de gegevensuitwisseling tussen aanbieders van gezondheidszorg. - Ga na in hoeverre zorginstellingen door middel van een risicoanalyse een gelaagdheid hebben aangebracht om het toepassingsgebied (scope) van het ISMS te bepalen. - Ga na of ook aandacht is voor e-Health toepassingen en bijvoorbeeld de rol van een afdeling klinische fysica & medische technologie (voor zover aanwezig).					
	4.4 Managementsysteem voor informatiebeveiliging	De organisatie moet een managementsysteem voor informatiebeveiliging inrichten, implementeren, onderhouden en continu verbeteren, in overeenstemming met de eisen van deze norm.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van documentatie op welke wijze de organisatie het ISMS heeft ingericht - Validatie van 1 proces/systeem om vast te stellen dat deze onderdeel uitmaakt van het ISMS					
5 Leiderschap	5.1 Leiderschap en betrokkenheid	De directie moet leiderschap en betrokkenheid tonen met betrekking tot het managementsysteem voor informatiebeveiliging door: a) te bewerkstelligen dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en aansluiten bij de strategische richting van de organisatie; b) te bewerkstelligen dat de eisen van het managementsysteem voor informatiebeveiliging in de processen van de organisatie worden geïntegreerd; c) te bewerkstelligen dat de voor het managementsysteem voor informatiebeveiliging benodigde middelen beschikbaar zijn; d) het belang van een doeltreffend informatiebeveiligingsmanagement en van het voldoen aan de eisen van het managementsysteem voor informatiebeveiliging te communiceren; e) te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt; f) mensen aan te sturen en te ondersteunen om een bijdrage te leveren aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging; g) continue verbetering te bevorderen; en h) andere relevante managementfuncties te ondersteunen om hun leiderschap te tonen binnen hun verantwoordelijkheidsgebieden.	- Interview met directie/management over: o het informatiebeveiligingsbeleid en de daarin geformuleerde doelstellingen; o de eisen die volgen uit het beleid worden geïntegreerd in de processen van de organisatie o ter beschikking stellen van de benodigde middelen; o het communiceren van het belang van een doeltreffend informatiebeveiligingsmanagement en van het voldoen aan de eisen van het managementsysteem. o het ondersteunen relevante managementfuncties om hun leiderschap binnen hun verantwoordelijkheidsgebied te tonen. - Inspectie van documentatie waarin de uitkomsten van bovenstaande activiteiten zijn gedocumenteerd.					
	5.2 Beleid	De directie moet een informatiebeveiligingsbeleid vaststellen dat: a) passend is voor het doel van de organisatie; b) informatiebeveiligingsdoelstellingen bevat (zie 6.2) of het kader biedt voor het vaststellen van informatiebeveiligingsdoelstellingen; c) een verbintenis bevat om te voldoen aan van toepassing zijnde eisen in verband met informatiebeveiliging; en d) een verbintenis bevat tot continue verbetering van het managementsysteem voor informatiebeveiliging. Het beleid voor informatiebeveiliging moet: e) beschikbaar zijn als gedocumenteerde informatie; f) worden gecommuniceerd binnen de organisatie, en g) beschikbaar zijn voor belanghebbenden, voor zover van toepassing.	- Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. - Ga na dat het informatiebeveiligingsbeleid is gedocumenteerd, gecommuniceerd en beschikbaar is voor belanghebbenden. - Inspectie van documentatie dat het Infomatiebeveiligingsbeleid door verantwoordelijk management is goedgekeurd. - Ga na dat het beleid periodiek en/of na grote wijzigingen opnieuw wordt vastgesteld.					
	5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie	De directie moet bewerkstelligen dat de verantwoordelijkheden en bevoegdheden voor rollen die relevant zijn voor informatiebeveiliging worden toegekend en gecommuniceerd. De directie moet de verantwoordelijkheid en bevoegdheid toekennen met betrekking tot: a) het bewerkstelligen dat het managementsysteem voor informatiebeveiliging voldoet aan de eisen van deze norm; en b) het rapporteren over de prestaties van het managementsysteem voor informatiebeveiliging aan de directie. OPMERKING De directie kan ook verantwoordelijkheden en bevoegdheden toekennen met betrekking tot het rapporteren over de prestaties van het managementsysteem voor informatiebeveiliging binnen de organisatie.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Deelwaarneming(en) op een aantal medewerkers dat rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie zijn gedocumenteerd en ingericht t.a.v. informatiebeveiliging. - Inspectie van een voortgangsrapportage t.a.v. informatiebeveiliging					
6 Planning	6.1 Maatregelen om risico's te beperken en kansen te benutten 6.1.1 Algemeen	Bij het plannen voor het managementsysteem voor informatiebeveiliging moet de organisatie de in 4.1 genoemde onderwerpen en de in 4.2 genoemde eisen overwegen, en de risico's en kansen vaststellen die moeten worden aangepakt om: a) te bewerkstelligen dat het managementsysteem voor informatiebeveiliging zijn beoogde resulta(a)t(en) behaalt; b) ongewenste effecten te voorkomen of te beperken; en c) continue verbetering te bereiken. De organisatie moet: d) maatregelen plannen om deze risico's te beperken en kansen te benutten; e) plannen op welke wijze: 1) de maatregelen in haar managementsysteemprocessen voor informatiebeveiliging worden geïntegreerd en geïmplementeerd; en 2) de doeltreffendheid van deze maatregelen moet worden geëvalueerd.	- Stel vast dat organisatie inzicht heeft in de vereisten, risico's en kansen voor informatiebeveiliging en maatregelen heeft gepland om deze in te vullen. - Interview met de verantwoordelijk functionaris(sen) over de wijze van borging dat het ISMS zijn beoogde doelstellingen behaalt en sprake is van continuë verbetering.					

	6.1.2 Risicobeoordeling van informatiebeveiliging	De organisatie moet een risicobeoordelingsprocedure voor informatiebeveiliging definiëren en toepassen die: a) risicocriteria voor informatiebeveiliging vaststelt en onderhoudt, waaronder: 1) de risicoacceptatiecriteria; en 2) criteria voor het verrichten van risicobeoordelingen van informatiebeveiliging; b) waarborgt dat herhaalde risicobeoordelingen van informatiebeveiliging consistente, geldige en vergelijkbare resultaten opleveren; c) de informatiebeveiligingsrisico's identificeert door: 1) het risicobeoordelingsproces voor informatiebeveiliging toe te passen om de risico's in verband met het verlies van vertrouwen in, integriteit van en beschikbaarheid van informatie binnen het toepassingsgebied van het managementsysteem voor informatiebeveiliging te identificeren; en 2) de risico eigenaren te identificeren; d) de informatiebeveiligingsrisico's analyseert door: 1) de potentiële gevolgen te beoordelen indien de risico's die in 6.1.2 c) 1) zijn vastgesteld, zich zouden voordoen; 2) de realistische waarschijnlijkheid te beoordelen van het voorkomen van de risico's die zijn vastgesteld in 6.1.2 c) 1); en 3) de risiconiveaus vast te stellen; e) de informatiebeveiligingsrisico's evalueert door: 1) de resultaten te vergelijken van risicoanalyses met de risicocriteria die zijn vastgesteld in 6.1.2 a); en 2) de geanalyseerde risico's te prioriteren voor risicobehandeling. De organisatie moet gedocumenteerde informatie bewaren over het risicobeoordelingsproces van informatiebeveiliging.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van documentatie van de risicobeoordelingsprocedure. - Deelwaarneming(en) op een risico beoordeling of de risicobeoordelingsprocedure is gevolgd resulterend in: o het gebruik van relevante dreigingen o het identificeren van de risico's o het afwegen van de risico's o het risico een eigenaar heeft					
	6.1.3 Behandeling van informatiebeveiligingsrisico's	De organisatie moet een behandelprocedure voor informatiebeveiligingsrisico's definiëren en toepassen om: a) passende opties voor het behandelen van informatiebeveiligingsrisico's te kiezen, rekening houdend met de resultaten van de risicobeoordeling; b) alle beheersmaatregelen vast te stellen die nodig zijn om de gekozen optie(s) voor het behandelen van informatiebeveiligingsrisico's te implementeren; OPMERKING Organisaties kunnen beheersmaatregelen naar behoefte ontwerpen of ze uit een bepaalde bron halen. c) de beheersmaatregelen die hiervoor in 6.1.3 b) zijn vastgesteld te vergelijken met die in bijlage A, en om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten; OPMERKING 1 Bijlage A bevat een uitgebreide lijst van beheersdoelstellingen en beheersmaatregelen. Gebruikers van deze norm worden verwezen naar bijlage A om te bewerkstelligen dat geen noodzakelijke beheersmaatregelen over het hoofd worden gezien. OPMERKING 2 Bij de gekozen beheersmaatregelen zijn beheersdoelstellingen impliciet begrepen. De in bijlage A opgesomde beheersdoelstellingen en beheersmaatregelen zijn niet uitputtend, en mogelijk zijn aanvullende beheersdoelstellingen en beheersmaatregelen nodig. d) een verklaring van toepasselijkheid op te stellen die bevat: — de benodigde beheersmaatregelen (zie 6.1.3 b) en c)); — een rechtvaardiging voor het opnemen ervan; — de informatie of de benodigde beheersmaatregelen zijn geïmplementeerd of niet, en — de rechtvaardiging voor het uitsluiten van in bijlage A genoemde beheersmaatregelen. e) een behandelplan voor informatiebeveiligingsrisico te formuleren; en f) van de risico eigenaren goedkeuring te verkrijgen voor het behandelplan voor informatiebeveiligingsrisico en acceptatie van de overblijvende informatiebeveiligingsrisico's. De organisatie moet gedocumenteerde informatie bewaren over de behandelprocedure van informatiebeveiligingsrisico's. OPMERKING De beoordelings en behandelprocedure van informatiebeveiligingsrisico's in deze norm is in overeenstemming met de principes en algemene richtlijnen in NEN ISO 31000.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van documentatie van de risicobehandelingsprocedure. - Deelwaarneming(en) op een risico beoordeling dat passende maatregelen zijn geïdentificeerd en geïmplementeerd. - Ga na dat organisatie de ingerichte maatregelen heeft vergeleken met bijlage A van NEN7510 deel 1 - Inspectie van documentatie van de VVT, die minimaal bevat: o de benodigde beheersmaatregelen (zie 6.1.3 b) en c)); o een rechtvaardiging voor het opnemen ervan; o de informatie of de benodigde beheersmaatregelen zijn geïmplementeerd of niet, en o de rechtvaardiging voor het uitsluiten van in bijlage A genoemde beheersmaatregelen. - Inspectie van het behandelplan, waarin de relatie is gelegd tussen het risico, de beheersmaatregel en het eventuele (geaccepteerde) restrisico.					
	6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken	De organisatie moet voor relevante functies en op relevante niveaus informatiebeveiligingsdoelstellingen vaststellen. De informatiebeveiligingsdoelstellingen moeten: a) consistent zijn met het informatiebeveiligingsbeleid; b) meetbaar zijn (indien praktisch uitvoerbaar); c) rekening houden met van toepassing zijnde informatiebeveiligingseisen en resultaten van risicobeoordeling en behandeling; d) worden gecommuniceerd; en e) indien van toepassing, worden geactualiseerd. De organisatie moet gedocumenteerde informatie over de informatiebeveiligingsdoelstellingen bewaren. Bij het opstellen van planningen voor het bereiken van de informatiebeveiligingsdoelstellingen moet de organisatie vaststellen: f) wat er moet worden gedaan; g) welke middelen er nodig zijn; h) wie er verantwoordelijk is; i) wanneer het moet zijn voltooid; en j) hoe de resultaten zullen worden geëvalueerd.	- Interview met de verantwoordelijk functionaris(sen) over de aansluiting tussen informatiebeveiligingsdoelstellingen en de strategische richting van de organisatie. - Ga na dat passende informatiebeveiligingsdoelstellingen zijn vastgesteld - Ga na op welke wijze wettelijke vereisten zijn meegenomen - Inspectie van documentatie/plannen voor het realiseren van de doelstellingen, waarbij er rekening gehouden wordt met het formaat en de complexiteit van de organisatie.					
7 Ondersteuning	7.1 Middelen	De organisatie moet de middelen vaststellen en beschikbaar stellen die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het managementsysteem voor informatiebeveiliging.	- Interview met de verantwoordelijk functionaris(sen) over dat voldoende middelen beschikbaar zijn gesteld voor het uitvoeren van de informatiebeveiligingsfunctie. - Ga bij geconstateerde afwijkingen t.o.v. de norm NEN 7510 na in hoeverre een tekort aan middelen een grondoorzaak kan zijn.					
	7.2 Competentie	De organisatie moet: a) de noodzakelijke competentie vaststellen van de perso(o)n(en) die onder haar gezag werkzaamheden verricht(en) die de prestaties van de organisatie op het gebied van informatiebeveiliging beïnvloeden; b) bewerkstelligen dat deze personen competent zijn op basis van de juiste scholing, opleiding of ervaring; c) waar van toepassing, maatregelen nemen om de benodigde competentie te verwerven, en de doeltreffendheid van de genomen maatregelen evalueren; en d) geschikte gedocumenteerde informatie als bewijsmateriaal van competentie bewaren. OPMERKING Geschikte maatregelen kunnen bijvoorbeeld zijn: het voorzien in training van, het begeleiden van, of het in een andere functie benoemen van mensen die al in dienst zijn; of het inhuren of contracteren van competente personen.	- Interview met de verantwoordelijk functionaris(sen) en ga na dat de organisatie: o heeft bepaald welke personen en hun competenties benodigd zijn voor het uitvoeren van informatiebeveiliging, zoals ze beschreven staan in functiebeschrijving of ISMS-beleidsdocumenten. o borgt dat de betreffende personen over deze competenties (komen te) beschikken. - Inspectie van documentatie waaruit blijkt dat relevante personen over de noodzakelijke competenties beschikken - Deelwaarneming(en) op deze personen in hoeverre over de noodzakelijke competenties wordt beschikt.					

	7.3 Bewustzijn	Personen die werkzaamheden verrichten onder het gezag van de organisatie, moeten zich bewust zijn van: a) het informatiebeveiligingsbeleid; b) hun bijdrage aan de doeltreffendheid van het managementsysteem voor informatiebeveiliging, met inbegrip van de voordelen van verbeterde informatiebeveiligingsprestaties; c) de gevolgen van het niet voldoen aan de eisen van het managementsysteem voor informatiebeveiliging.	- Interview met de verantwoordelijk functionaris(sen) over in hoeverre zij bekend zijn met het informatiebeveiligingsbeleid - Inspectie van maatregelen/documentatie waaruit blijkt dat de organisatie periodiek aandacht geeft aan het creëren van bewustzijn bij medewerkers rondom IB - Ga na dat medewerkers hebben ingestemd met de organisatie vereisten t.a.v. informatiebeveiliging, bijvoorbeeld door ontvangst/ondertekening van de gedragscode - Inspectie van de werkplek(ken) om vast te stellen in hoeverre medewerkers zich houden aan de organisatie vereisten t.a.v. informatiebeveiliging.					
	7.4 Communicatie	De organisatie moet de behoefte vaststellen aan interne en externe communicatie die relevant is voor het managementsysteem voor informatiebeveiliging, waaronder: a) waarover te communiceren; b) wanneer te communiceren; c) met wie te communiceren; d) wie moet communiceren; en e) volgens welke processen de communicatie moet plaatsvinden.	- Interview met de verantwoordelijk functionaris(sen) op welke wijze de behoefte aan interne en externe communicatie over informatiebeveiliging is geïnventariseerd en gedocumenteerd in bijvoorbeeld een communicatieplan. - Inspectie van documentatie zoals het communicatieplan en de resultaten van uitgevoerde communicatie activiteiten.					
	7.5 Gedocumenteerde informatie 7.5.1 Algemeen	Het managementsysteem voor informatiebeveiliging van de organisatie moet onder andere bevatten: a) gedocumenteerde informatie die deze norm vereist; en b) de gedocumenteerde informatie die de organisatie vaststelt als noodzakelijk voor de doeltreffendheid van het managementsysteem voor informatiebeveiliging. OPMERKING De uitgebreidheid van gedocumenteerde informatie voor een managementsysteem voor informatiebeveiliging kan van organisatie tot organisatie verschillen vanwege: 1) de omvang van de organisatie en het type van haar activiteiten, processen, producten en diensten; 2) de complexiteit van de processen en hun interacties; en 3) de competentie van de mensen.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van de gedocumenteerde informatie van het managementsysteem voor informatiebeveiliging conform vereisten van deze norm.					
	7.5.2 Creëren en actualiseren	Bij het creëren en actualiseren van gedocumenteerde informatie moet de organisatie zorgen voor de/het passende: a) identificatie en beschrijving (bijv. een titel, datum, auteur of referentienummer); b) format (bijv. taal, softwareversie, afbeeldingen) en media (bijv. papier, elektronisch); en c) beoordeling en goedkeuring van geschiktheid en adequaatheid.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Deelwaarneming(en) op documentatie van het management systeem dat deze conform documentvereisten van de organisatie zijn.					
	7.5.3 Beheer van gedocumenteerde informatie	Gedocumenteerde informatie zoals het managementsysteem voor informatiebeveiliging en deze norm vereisen, moet worden beheerd om te bewerkstelligen dat: a) de informatie beschikbaar is en geschikt is voor gebruik, waar en wanneer het nodig is; b) de informatie adequaat is beveiligd (bijv. tegen verlies van vertrouwelijkheid, oneigenlijk gebruik en aantasting). Voor het beheren van gedocumenteerde informatie moet de organisatie, voor zover van toepassing, invulling geven aan de volgende activiteiten: c) distributie, toegang, het terugvinden alsmede het gebruik; d) opslag en behoud, waaronder behoud van leesbaarheid; e) beheersing van wijzigingen (bijv. versiebeheer); en f) bewaring en vernietiging. Gedocumenteerde informatie van externe oorsprong die de organisatie nodig acht voor de planning en uitvoering van het managementsysteem voor informatiebeveiliging, moet worden geïdentificeerd voor zover van toepassing en beheerd. OPMERKING Toegang betekent een besluit tot toestemming om de gedocumenteerde informatie alleen in te zien, of tot toestemming en bevoegdheid om de gedocumenteerde informatie in te zien en te wijzigen, enz.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van de document beheerprocedures. - Deelwaarneming(en) op documentatie dat deze conform de vastgestelde beheerprocedures wordt bewaard, gedistribueerd, gewijzigd, gepubliceerd, etc.					
8 Uitvoering	8.1 Operationele planning en beheersing	Om te voldoen aan de informatiebeveiligingseisen en om de in 6.1 vastgestelde maatregelen te implementeren moet de organisatie de benodigde processen plannen, implementeren en beheersen. De organisatie moet ook plannen implementeren om de in 6.2 vastgestelde informatiebeveiligingsdoelstellingen te bereiken. De organisatie moet gedocumenteerde informatie bijhouden in de omvang die nodig is om het vertrouwen te hebben dat de processen volgens planning zijn uitgevoerd. De organisatie moet geplande wijzigingen beheersen en de consequenties van onbedoelde wijzigingen beoordelen, en zo nodig maatregelen treffen om nadelige effecten tegen te gaan. De organisatie moet bewerkstelligen dat uitbestede processen worden vastgesteld en beheerst.	- Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. - Deelwaarneming(en) dat processen, doelstellingen, acties en maatregelen volgens planning zijn/worden uitgevoerd/geïmplementeerd - Deelwaarneming(en) dat wijzigingen op beheerste wijze worden doorgevoerd en eventuele nadelige gevolgen van wijzigingen worden gemitigeerd. - Inspectie van documentatie dat de organisatie uitbestede processen heeft vastgesteld en beheerst (zie ook A.15 NEN 7510-2)					
	8.2 Risicobeoordeling van informatiebeveiliging	De organisatie moet risicobeoordelingen van informatiebeveiliging met geplande tussenpozen uitvoeren, of als significante veranderingen worden voorgesteld of zich voordoen, rekening houdend met de criteria die zijn vastgesteld in 6.1.2 a). De organisatie moet gedocumenteerde informatie bewaren van de resultaten van de risicobeoordelingen van informatiebeveiliging.	- Inspectie van risicobeoordelingen dat deze met geplande tussenpozen of bij significante wijzigingen opnieuw worden uitgevoerd. - Interview met de verantwoordelijk functionaris(sen) over op welke wijze de risicobeoordelingen (opnieuw) worden uitgevoerd.					
	8.3 Informatiebeveiligingsrisico's behandelen	De organisatie moet het behandelplan van informatiebeveiligingsrisico's implementeren. De organisatie moet gedocumenteerde informatie bewaren van de resultaten van het behandelen van informatiebeveiligingsrisico's.	- Inspectie van documentatie dat beoogde maatregelen uit het behandelplan volgens planning zijn geïmplementeerd. - Interview met de verantwoordelijk functionaris(sen) om de resultaten van het behandelplan te bespreken.					
9 Evaluatie van de prestaties	9.1 Monitoren, meten, analyseren en evalueren	De organisatie moet de informatiebeveiligingsprestaties en de doeltreffendheid van het managementsysteem voor informatiebeveiliging evalueren. De organisatie moet vaststellen: a) wat moet worden gemonitord en gemeten, met inbegrip van informatiebeveiligingsprocessen en beheersmaatregelen; b) welke methoden worden toegepast voor het, voor zover van toepassing, monitoren, meten, analyseren en evalueren, om geldige resultaten te bewerkstelligen; OPMERKING De gekozen methoden behoren vergelijkbare en reproduceerbare resultaten op te leveren om als geldig te worden beschouwd. c) wanneer moet worden gemonitord en gemeten; d) wie moet monitoren en meten; e) wanneer de resultaten van het monitoren en meten moeten worden geanalyseerd en geëvalueerd; en f) wie deze resultaten moet analyseren en evalueren. De organisatie moet geschikte gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten van het monitoren en meten.	- Inspectie van documentatie op welke wijze de organisatie de prestaties en doeltreffendheid van het ISMS monitort/evalueert - Interview met de verantwoordelijk functionaris(sen) om bestaan van meten/evalueren vast te stellen overeenkomstig de gedefinieerde vereisten.					

	9.2 Interne audit	De organisatie moet met geplande tussenpozen interne audits uitvoeren om informatie te verkrijgen of het managementsysteem voor informatiebeveiliging: a) overeenkomt met: 1) de eigen eisen van de organisatie voor haar managementsysteem voor informatiebeveiliging; en 2) de eisen van deze norm; b) doeltreffend is geïmplementeerd en onderhouden. De organisatie moet: c) (een) auditprogramma('s) plannen, vaststellen, implementeren en onderhouden, met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage. Het auditprogramma moet rekening houden met het belang van de betrokken processen en de resultaten van voorgaande audits; d) de auditcriteria voor en de reikwijdte van elke audit definiëren; e) auditoren selecteren en audits uitvoeren zodanig dat de objectiviteit en de onpartijdigheid van het auditproces worden bewerkstelligd; f) bewerkstelligen dat de resultaten van de audits worden gerapporteerd aan het relevante management; en g) gedocumenteerde informatie bewaren als bewijsmateriaal van het auditprogramma en de auditresultaten.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van documentatie dat een plan of programma voor (interne) audits is vastgesteld. - Ga na of de verantwoordelijk functionaris(sen) voor het uitvoeren van de interne audits over de juiste competenties beschikken waaronder onpartijdigheid, deskundigheid en objectiviteit. - Inspectie van documentatie dat organisatie regelmatig (interne) audits uitvoert om informatie te verkrijgen over het functioneren van het managementsysteem voor informatiebeveiliging.					
	9.3 Directiebeoordeling	De directie moet met geplande tussenpozen het managementsysteem voor informatiebeveiliging van de organisatie beoordelen, om de continue geschiktheid, adequaatheid en doeltreffendheid te bewerkstelligen. Bij de directiebeoordeling moet onder andere in overweging worden genomen: a) de status van acties als gevolg van voorgaande directiebeoordelingen; b) wijzigingen in externe en interne onderwerpen die relevant zijn voor het managementsysteem voor informatiebeveiliging; c) feedback over de informatiebeveiligingsprestaties, met inbegrip van trends in: 1) afwijkingen en corrigerende maatregelen; 2) resultaten van monitoren en meten; 3) auditresultaten; en 4) voldoen aan informatiebeveiligingsdoelstellingen; d) feedback van belanghebbenden; e) resultaten van risicobeoordeling en de status van het risicobehandelplan; en f) kansen voor continue verbetering. De resultaten van de directiebeoordeling moeten beslissingen omvatten met betrekking tot kansen voor continue verbetering en de noodzaak voor wijzigingen in het managementsysteem voor informatiebeveiliging. De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van de resultaten van de directiebeoordeling.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van documentatie waaruit blijkt dat de directie periodiek beoordelingen uitvoert om vast te stellen dat IB processen en maatregelen effectief functioneren. - Inspectie van documentatie waaruit blijkt dat directie wordt geïnformeerd over de status van acties, geplande maatregelen, doelstellingen, afwijkingen en wijzigingen. - Ga na dat de directie beslissingen neemt mbt kansen voor verbetering of wijzigingen aan het ISMS. - Interview verantwoordelijk RvB-lid/ directie in hoeverre zij geïnformeerd worden en besluiten nemen over informatiebeveiliging.					
10 Verbetering	10.1 Afwijkingen en corrigerende maatregelen	Wanneer zich een afwijking voordoet, moet de organisatie: a) op de afwijking reageren, en indien van toepassing: 1) maatregelen treffen om de afwijking te beheersen en te corrigeren; en 2) de consequenties aanpakken; b) de noodzaak evalueren om maatregelen te treffen om de oorzaken van de afwijking weg te nemen, zodat de afwijking zich niet herhaalt of zich elders voordoet, door: 1) de afwijking te beoordelen; 2) de oorzaken van de afwijking vast te stellen; en 3) vast te stellen of zich gelijksoortige afwijkingen voordoen of zouden kunnen voordoen; c) de benodigde maatregelen implementeren; d) de doeltreffendheid van getroffen corrigerende maatregelen beoordelen; e) zo nodig, wijzigingen aanbrengen in het managementsysteem voor informatiebeveiliging. Corrigerende maatregelen moeten passend zijn voor de effecten van de opgetreden afwijkingen. De organisatie moet gedocumenteerde informatie bewaren als bewijsmateriaal van: f) de aard van de afwijkingen en de vervolgens genomen maatregelen; en g) de resultaten van corrigerende maatregelen.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van de incidenten registratie. - Deelwaarneming(en) op de incidentenregistratie dat een oorzaak analyse is uitgevoerd en heeft geleid tot verbeteringen in het ISMS in dien van toepassing.					
	10.2 Continue verbetering	De organisatie moet continu de geschiktheid, adequaatheid en doeltreffendheid van het managementsysteem voor informatiebeveiliging verbeteren.	- Interview met de verantwoordelijk functionaris(sen) over opzet/bestaan van geïmplementeerde maatregelen. - Inspectie van het verbeterregister dat verbeteracties zijn geïdentificeerd, gepland en uitgevoerd.					

Gedragslijn 2.0 aandachtsgebied	Referentie NEN 7510-1:2017	Beheersmaatregel NEN 7510-1:2017 Annex A	Criteria Gedragslijn 2.0	Testaanpak (hulpmiddel voor self-assessment)	Resultaat opzet	Resultaat bestaan	Bevindingen	Acties	Evidence
Beheer van bedrijfsmiddelen	A.8.1.1 Inventariseren van bedrijfsmiddelen	Beheersmaatregel (bron: NEN 7510-1 annex A) Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatieverwerkende faciliteiten, moeten worden geïdentificeerd, en van deze bedrijfsmiddelen moet een inventaris worden opgesteld en onderhouden. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten: a) verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen); b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen; c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	a) De organisatie heeft beleid voor de classificatie met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid van de informatie en bepaalt afhankelijk daarvan het belang van bedrijfsmiddelen die persoonlijke gezondheidsinformatie bevatten.	· Inspectie van het classificatie beleid. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van het beleid.					
			b) De organisatie heeft de bedrijfsmiddelen, waaronder ook e-Health toepassingen vallend onder de Wet Medische Hulpmiddelen, conform het beleid geïnventariseerd en geclassificeerd, waarbij voor elk in de inventarisatie opgenomen bedrijfsmiddel een verantwoordelijke (eigenaar) is vastgesteld. Dit kan ook een derde partij zijn.	· Inspectie van het register van bedrijfsmiddelen (CMDB) · Deelwaarneming(en) op het CMDB of bedrijfsmiddelen conform het beleid zijn geclassificeerd (gericht op software), waaronder het vaststellen van een eigenaar.					
			c) De organisatie heeft de aanschaf en het gebruik van bedrijfsmiddelen, apparatuur en software, waaronder e-Health toepassingen, beoordeeld op relevante privacy- en informatiebeveiligingsaspecten en hierop passende maatregelen getroffen.	· Deelwaarneming(en) dat relevante bedrijfsmiddelen zijn beoordeeld op relevante privacy- en informatiebeveiligingsaspecten.					
			d) De organisatie zorgt dat de classificatie en inventarisatie actueel zijn.	· Inspectie van het register van bedrijfsmiddelen (CMDB)					
			e) De organisatie beschikt over regels voor het aanvaardbare gebruik van deze bedrijfsmiddelen.	· Inspectie van de regels voor het aanvaardbare gebruik van deze bedrijfsmiddelen, zoals een gebruikersovereenkomst of een gedragscode.					
			f) De organisatie zorgt voor een juiste gang van zaken als het bedrijfsmiddel wordt verwijderd of vernietigd.	· Inspectie van het verwijder/vernietig protocol. · Deelwaarneming of een bedrijfsmiddel conform protocol is verwijderd/vernietigd.					
Cyber Security	A.6.2.2 Telewerken	Beheersmaatregel (bron: NEN 7510-1 annex A) Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie heeft richtlijnen en procedures voor telewerken opgesteld en geïmplementeerd. De richtlijnen behandelen onder andere het veilig werken buiten kantoorlocaties (inclusief beveiliging eigen werkplek), het inrichten van MFA en clean desk/clear screen policy thuis, het veilig delen van data (risico van meekijken en meeluisteren huisgenoten) en het verantwoord virtueel samenwerken.	· Inspectie van het de richtlijnen/procedures. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van het de ingerichte richtlijnen/procedures. · Inspectie van bewustzijnsmiddelen en -activiteiten (zie A.7.2.2)					
			b) De organisatie hanteert voor externe toegang tot systemen die persoonlijke gezondheidsinformatie bevatten passende beveiligde (versleutelde) verbindingen en MFA.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van de ingerichte maatregelen. · Deelwaarneming(en) op de externe toegang/verbindingen dat deze conform beleid zijn ingericht.					
			c) De organisatie besteedt aandacht aan bewustzijnsactiviteiten rondom het veilig werken buiten kantoorlocaties, het inrichten van MFA en clean desk/clear screen policy thuis, het veilig delen van data en verantwoord virtueel samenwerken.	· Inspectie van bewustzijnsmiddelen en -activiteiten (zie A.7.2.2)					
			d) De organisatie bevordert de naleving van richtlijnen en procedures voor telewerken, bijvoorbeeld door aandacht te geven aan informatiebeveiligingsbewustzijn bij telewerken, afdwingen van MFA bij inloggen, het activeren van schermbeveiliging na een periode van inactiviteit, het monitoren op gebruik van veilige voorzieningen voor het delen van data en virtueel samenwerken.	· Inspectie van bewustzijnsmiddelen en -activiteiten (zie A.7.2.2 en vorige cel) · Inspectie van ingerichte maatregelen.					
	A.12.2.1 Bescherming tegen malware	Beheersmaatregel (bron: NEN 7510-1 annex A) Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers. - - Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie , detectie en responsbeheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software en moeten passende bewustzijnstraining voor gebruikers implementeren.	a) De organisatie heeft actuele beschermingsmaatregelen getroffen om kwaadaardige software (waaronder virus, spyware en andere malware) te detecteren en de gevolgen hiervan te mitigeren door middel van bijvoorbeeld anti-virus en anti-malware software, endpoint protection, whitelisting, een Security Operations Center (SOC), een Intrusion Detection System (IDS) en/of een Intrusion Prevention System (IPS).	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Ga na of de organisatie heeft vastgesteld dat de combinatie van ingerichte maatregelen, zoals virusscanner, anti spy- en malware, etc de onderliggende risico's in voldoende mate heeft geaddresseerd.					
			b) De organisatie houdt de beschermingsmaatregelen up-to-date conform de nieuwste definities en inzichten en logt detectie en verwijdering van kwaadaardige software.	· Deelwaarneming(en) op de toepassing van de laatste definities in virusscanner, anti spy- en malware, etc. · Ga voor 1 voorbeeld na of kwaadaardige software is gedetecteerd en verwijderd.					
			c) De organisatie evalueert periodiek de werking van de beschermingsmaatregelen.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen.					
			d) De organisatie herstelt waar nodig de negatieve gevolgen van kwaadaardige software en andere inbreuken.	· Deelwaarneming(en) van de afhandeling van een incident gerelateerd aan kwaadaardige software of andere inbreuken conform afgesproken procedures (zie A.16.1.5).					
			e) De organisatie informeert de gebruikers over schadelijke software en mogelijke risico's, hoe zij hiermee in aanraking kunnen komen (phishing mails, bijlagen bij e-mails, e.d.), wat zij kunnen doen om inbreuken door deze software te voorkomen en hoe zij inbreuken moeten melden.	· Inspectie van bewustzijnsmiddelen en -activiteiten (zie A.7.2.2) · Inspectie van procedures om verdachte software en vermeende inbreuken te melden (zie A.16.1.2)					
	A.12.6.1 Beheer van technische kwetsbaarheden	Beheersmaatregel (bron: NEN 7510-1 annex A) Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt, moet tijdig worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt, aan te pakken. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie bepaalt periodiek (zo nodig dagelijks) en bij voorkeur door middel van geautomatiseerde vulnerability scanning tools de kwetsbaarheden binnen de in gebruik zijnde informatiesystemen, onderliggende infrastructuur en netwerken.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van ingerichte maatregelen, zoals vulnerability scanning tools, etc.					
			b) De organisatie heeft een proces ingericht om tijdig alerts te ontvangen. De ontvangen alerts worden geëvalueerd en indien nodig tijdig opgevolgd.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van proces/procedure voor afhandelen alerts, bijvoorbeeld meldingen Z-CERT.					
			c) Algemene ontwikkelingen op het gebied van security worden gemonitord, door bijvoorbeeld kennis te nemen van Z-CERT alerts, NCSC-informatiebulletins en security nieuws die op andere websites worden gepubliceerd (SANS, Tweakers, Security.NL, etc.).	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van proces/procedure voor afhandelen alerts, bijvoorbeeld meldingen Z-CERT.					
			d) De organisatie neemt tijdig (zo nodig acuut) maatregelen (zoals patchmanagement) om de kwetsbaarheden weg te nemen en/of om de risico's zo veel als mogelijk te beperken.	· Inspectie van het patch management proces. · Deelwaarneming(en) op servers, firewalls, besturingssystemen etc of de laatste patches zijn geïnstalleerd volgens het vastgestelde proces.					
	A.13.1.3 scheiding in netwerken	Beheersmaatregel (bron: NEN 7510-1 annex A) Groepen van informatiediensten, gebruikers en systemen moeten in netwerken worden gescheiden. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden, hierbij wordt in het bijzonder aandacht besteed aan die netwerkonderdelen waar medische apparatuur is gekoppeld aan het netwerk.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van beleid/ontwerp voor netwerkzonering en koppelvlakken incl. gehanteerde ontwerpprincipes (al dan niet als onderdeel van bovenliggende netwerkarchitectuur).					
			b) Segmentering maakt het mogelijk om groepen van servers en informatiesystemen logisch of fysiek van elkaar te scheiden, waarbij het doel is om de impact van een beveiligingsincident te beperken tot het segment waar dit plaatsvindt. Voorbeelden van segmentering ter overweging zijn: • Afgescheiden DMZ • Afgescheiden beheernetwerk • Gescheiden netwerk medische apparatuur met remote support • Gescheiden netwerk verouderde apparatuur (Windows XP, 7, 8) • Gescheiden wifi-netwerken (restricted voor eigen, public voor anderen) • Scheiden naar OTAP	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van beleid/ontwerp voor netwerkzonering en koppelvlakken incl. gehanteerde ontwerpprincipes (al dan niet als onderdeel bovenliggende netwerkarchitectuur).					
			c) De organisatie beschikt over beleid waarin is vastgelegd welke uitgangspunten voor segmentering zijn gehanteerd en welke koppelvlakken zijn ingericht.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van beleid/ontwerp voor netwerkzonering en koppelvlakken.					
			d) Alle gescheiden groepen hebben een beveiligingsniveau dat refereert aan de classificatie en het beleid van de organisatie.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Ga na hoe de relatie is gelegd tussen de (gegevens) classificatie enerzijds en het beleid/inrichting van zonering anderzijds.					
			e) Van informatiesystemen en servers wordt bijgehouden in welk segment ze staan. Dit overzicht dient actueel te zijn.	· Inspectie van het register van bedrijfsmiddelen. · Deelwaarneming(en) op het register van bedrijfsmiddelen dat servers conform het beleid zijn gezoneerd.					

	A.14.2.3 technische beoordeling van toepassingen na wijzigingen besturingsplatform	Beheersmaatregel (bron: NEN 7510-1 annex A) Als besturingsplatforms zijn verandert, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie voert bij het implementeren van wijzigingen in (besturings)systemen die impact kunnen hebben op informatiebeveiliging/ privacy, vooraf een risicoanalyse en -beoordeling uit om de effecten op de (bedrijfsgevoelige) informatiesystemen in kaart te brengen.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van het wijzigingsbeheerproces - stel vast dat in daarvoor in aanmerking komende situaties daadwerkelijk een passende risicoanalyse is uitgevoerd						
			b) De organisatie test de wijzigingen in (besturings)systemen van bedrijfskritieke toepassingen, indien mogelijk in de testomgeving, en geeft de wijziging pas vrij nadat de testresultaten akkoord zijn bevonden.	· Deelwaarneming(en) op doorgevoerde wijzigingen of deze conform het wijzigingsbeheerproces zijn doorgevoerd.						
			c) Als het beleid inzake pentesten of de uitgevoerde risicoanalyse daartoe aanleiding geeft, voert de organisatie een penetratietest uit (zie A.18.2.3).	· Deelwaarneming(en) op doorgevoerde wijzigingen of indien nodig een penetratietest is uitgevoerd.						
	A.18.2.3 Beoordeling van technische naleving	Beheersmaatregel (bron: NEN 7510-1 annex A) Informatiesystemen moeten regelmatig worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) Ten minste jaarlijks en na grote wijzigingen wordt een penetratietest uitgevoerd op ten minste alle externe koppelvlakken die met internet zijn verbonden (internet-facing systemen). Overweeg vanwege onafhankelijkheid en deskundigheid om een externe partij in te schakelen. Neem in de scope de volgende onderwerpen mee ter overweging: • DNSSEC en TLS; • NCSC webapplicatie richtlijnen U/PW.02, U/PW.03, U/WA.03, U/WA.04. NB deze zijn voor DigiD assessments al verplicht; • Domeinen die gelinkt kunnen worden aan de naam van de zorginstelling; • Het kunnen aansluiten van niet-organisatie apparatuur op de netwerkaansluitingen binnen de locatie van de zorginstelling.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van de jaarplanning voor technische beoordelingen / penetratietesten. · Inspectie van de resultaten van de uitgevoerde pentesten en de opvolging van bevindingen. · Ga na of de scope van de penetratietesten is gericht op de hoog risico gebieden zoals externe koppelvlakken en genoemde onderwerpen ter overweging zijn meegenomen.						
			b) De hoogrisicobevindingen uit de rapportage van de penetratietest worden direct gemitigeerd en voor de midden-/laagrisicobevindingen wordt een planning gemaakt om deze met inachtneming van de zwaarte van het risico te mitigeren.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Ga na hoe de opvolging van hoog/medium/laag risico bevindingen conform vereisten is geborgd. Check bijvoorbeeld of de geconstateerde bevindingen zijn opgenomen in het ISMS voor monitoring van de opvolging.						
Leveranciersmanagement	A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Beheersmaatregel (bron: NEN 7510-1 annex A) Alle relevante informatiebeveiligingseisen moeten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie beschikt over beleid en/of richtlijnen wie verantwoordelijk is voor welk onderdeel van leveranciersmanagement. Denk hierbij aan het opstellen van een PVE, contacten met leveranciers (Inkoop), bewaren en bewaken (geldigheid) overeenkomsten (Inkoop), bewaken levering conform niveaus SLA (afnemende afdelingen), bewaken informatiebeveiliging (certificeringen, TPM/SOC, e.d.).	· Inspectie van het beleid en/of richtlijnen voor leveranciersmanagement. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van het beleid en/of richtlijnen.						
			b) De organisatie voert voor het aanschaffen en invoeren van een product of dienst met impact op persoonlijke gezondheidsinformatie, waaronder tevens inbegrepen e-Health toepassingen, een classificatie en/of risicoanalyse uit op minimaal de informatiebeveiligings en privacyvereisten. Op basis van de uitkomsten van de classificatie en/of risicoanalyse zijn beheersmaatregelen geselecteerd en worden deze als aanvullende vereisten vastgelegd in het contract en/of SLA.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van het inkoopproces/procedure · Deelwaarneming(en) op gecontracteerde leveranciers om vast te stellen of aan vereisten is voldaan.						
			c) Indien de leverancier een verwerker is van gegevens conform de definitie van de AVG, voert de verwerkingsverantwoordelijke indien noodzakelijk een DPIA uit. De organisatie komt waar nodig een verwerkersovereenkomst overeen en/ of legt aanvullende vereisten vast in het contract en/of SLA. Aandachtspunt hierbij is het zorgen voor een consistente en eventueel getrapte uitwerking zodat onduidelijkheden en inconsistentie worden voorkomen (SLA/DAP bevatten alleen nadere uitwerkingen).	· Inspectie van het inkoopproces/procedure · Deelwaarneming(en) op gecontracteerde leveranciers om vast te stellen of aan vereisten is voldaan.						
			d) De organisatie maakt afspraken met de leverancier op welke wijze de leverancier aantoonbaar voldoet aan de gestelde vereisten, bijvoorbeeld door middel van periodiek overleg, SLA-rapportages en (third party) assurance verklaringen (TPM/SOC2).	· Inspectie van het inkoopproces/procedure · Deelwaarneming(en) op gecontracteerde leveranciers om vast te stellen of aan vereisten is voldaan.						
			e) Specifiek voor de aanschaf en het gebruik van e-Health toepassingen en Medische Technologie heeft de organisatie aandacht voor de belangrijkste risico's die verbonden zijn aan de (huidige en toekomstige) omgeving voor ICT/e-Health toepassingen. De organisatie heeft maatregelen getroffen om deze risico's te beheersen. Daarbij is rekening gehouden met aspecten als patiëntveiligheid, zorgcontinuïteit en informatiebeveiliging: • De organisatie brengt de risico's van de huidige (en eventueel toekomstige) ICT/toepassingen in kaart. • De organisatie heeft rekening gehouden met verschillende aspecten, zoals zorgcontinuïteit, informatiebeveiliging en patiëntveiligheid, waaronder medicatieveiligheid. • Als de organisatie belangrijke risico's heeft gevonden, dan wordt actie ondernomen om deze te beheersen.	· Inspectie van het inkoopproces/procedure · Deelwaarneming(en) op gecontracteerde leveranciers om vast te stellen of aan vereisten is voldaan.						
	A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	Beheersmaatregel (bron: NEN 7510-1 annex A) Organisaties moeten regelmatig de dienstverlening van leveranciers monitoren, beoordelen en auditen. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie controleert en beoordeelt periodiek de dienstverlening door externe partijen.	· Inspectie van het beleid en/of richtlijnen voor leveranciersbeoordeling. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van het beleid en/of richtlijnen. · Deelwaarneming(en) op gecontracteerde leveranciers om vast te stellen of aan vereisten is voldaan.						
			b) De organisatie bewaakt en controleert of het product, de dienst en de leverancier blijvend voldoen aan de gemaakte afspraken. Bij constatering van afwijkingen meldt de organisatie dit schriftelijk aan de leverancier en monitort de opvolging door de leverancier (bijvoorbeeld door vastlegging als actiepunt in de notulen van periodiek overleg).	· Deelwaarneming(en) op gecontracteerde leveranciers om vast te stellen of aan vereisten is voldaan.						
			c) Indien in de overeenkomst vaste evaluatiemomenten, audits of third party assurance verklaringen zijn opgenomen, bewaakt de organisatie dat deze activiteiten daadwerkelijk plaatsvinden en de uitkomsten worden geanalyseerd in relatie tot de uitgevoerde risicoanalyses. Acties ter verbetering worden uitgevoerd.	· Deelwaarneming(en) op gecontracteerde leveranciers om vast te stellen of aan vereisten is voldaan.						
Beheer van informatiebeveiligingsincidenten	A.16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen	Beheersmaatregel (bron: NEN 7510-1 annex A) Informatiebeveiligingsgebeurtenissen moeten zo snel mogelijk via de juiste leidinggevende niveaus worden gerapporteerd. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen: 1.ØM een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen; 2.ØM te garanderen dat er een doeltreffend en geprioriteerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement; 3.ØM incidentgerelateerde auditverslagen en ander relevant bewijs te verzamelen en in stand te houden. Informatiebeveiligingsincidenten omvatten corruptie of onbedoelde openbaarmaking van persoonlijke gezondheidsinformatie of het niet langer beschikbaar zijn van gezondheidsinformatiesystemen waarbij dit niet beschikbaar zijn nadelige gevolgen heeft voor de zorg voor cliënten of bijdraagt aan nadelige klinische gebeurtenissen. Organisaties moeten de cliënt altijd informeren als er per ongeluk persoonlijke gezondheidsinformatie openbaar is gemaakt. Organisaties moeten de cliënt op de hoogte stellen als het niet beschikbaar zijn van gezondheidsinformatiesystemen negatieve gevolgen gehad kan hebben voor hun zorgverlening.	a) Medewerkers zijn gewezen op hun verantwoordelijkheid om informatiebeveiligingsgebeurtenissen zo snel mogelijk te rapporteren en zijn geïnformeerd over de procedure voor het melden van informatiebeveiligingsgebeurtenissen.	· Inspectie van het beleid voor informatiebeveiliging en/of gedragscode · Inspectie van de procedure voor het melden van informatiebeveiligingsgebeurtenissen (NB het melden van datalekken mag via hetzelfde proces verlopen).						
			b) De organisatie heeft procedures voor het melden en classificeren van informatiebeveiligingsincidenten.	· Inspectie van de procedure voor het melden en afhandelen van informatiebeveiligingsgebeurtenissen.						

			c) De organisatie handelt geconstateerde incidenten volgens een vaste procedure af. In deze procedure is aandacht besteed aan de volgende vereisten: • identificatie van (de impact van) het incident; • vaststelling van de (basis-)oorzaak van het incident; • het uitvoeren van de gevolganalyse, bestaande uit o.a.: i. corrigeren van het incident (al dan niet met een tijdelijke work-around), ii. evalueren van de noodzaak voor maatregelen om zeker te stellen dat het incident niet opnieuw optreedt, iii. vaststellen van de benodigde maatregelen voor het tijdig implementeren van correctieve maatregelen, iv. vastleggen van de resultaten van uitgevoerde maatregelen en v. beoordelen van de effectiviteit van correctieve maatregelen.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Deelwaarneming(en) op het informatiebeveiligingsincident proces om vast te stellen of aan de vereisten is voldaan.					
			d) De organisatie hanteert een procedure voor het indien noodzakelijk informeren van de patiënt en eventuele toezichthouders.	· Inspectie van de datalek procedure.					
	A.16.1.5 Respons op informatiebeveiligingsincidenten	Beheersmaatregel (bron: NEN 7510-1 annex A) Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie beschikt over procedures voor de afhandeling van informatiebeveiligingsincidenten op basis van (de classificatie van) het incident en de daarbij behorende escalatieniveaus en escalatiepaden.	· Inspectie van de procedure voor het melden en afhandelen van informatiebeveiligingsgebeurtenissen. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen.					
			b) De organisatie houdt een registratie bij van gerapporteerde informatiebeveiligingsincidenten, de hieraan gegeven opvolging en de evaluatie van de effectiviteit van bestaande c.q. bijgestelde beheersmaatregelen.	· Inspectie van de registratie van informatiebeveiligingsgebeurtenissen.					
	A.16.1.6 Lering uit informatiebeveiligingsincidenten	Beheersmaatregel (bron: NEN 7510-1 annex A) Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen, moet worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) Periodieke effectevaluatie vindt plaats om combinaties van verschillende incidenten en/of terugkerende of ingrijpende incidenten te identificeren.	· Inspectie van de analyse op informatiebeveiligingsgebeurtenissen. · Interview met de verantwoordelijk functionaris(sen) over het lerend vermogen.					
			b) De effectiviteit van bestaande risicoanalyses en beheersmaatregelen wordt op basis van de analyse geëvalueerd, waar nodig bijgesteld en aan het verantwoordelijk management gerapporteerd.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen.					
			c) De organisatie gebruikt waar relevant de uitkomsten van de uitgevoerde evaluaties om het informatieveiligheidsbewustzijn van medewerkers te bevorderen.	· Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. · Inspectie van bewustzijnsmiddelen en -activiteiten					
Continuïteitsbeheer	A.17.1.2 Informatiebeveiligingscontinuïteit implementeren	Beheersmaatregel (bron: NEN 7510-1 annex A) De organisatie moet processen, procedures en beheersmaatregelen vaststellen, documenteren, implementeren en handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie beschikt over beleid, richtlijnen en procedures om de continuïteit van de informatievoorziening te waarborgen, al dan niet als onderdeel van crisisplannen annex de crisisorganisatie. Gebruik externe bronnen als input (zoals het rapport van de Onderzoeksraad voor de veiligheid).	· Inspectie van het beleid, richtlijnen en procedures voor continuïteitswaarborging. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. Zie voor best practice aanbevelingen het onderzoeksrapport van de OvV.					
			b) Met het oog op een goede voorbereiding op de uitval van ICT, brengt de organisatie de afhankelijkheden tussen zorg en ICT periodiek in kaart, inclusief de mogelijke risico's voor patiënten die gepaard gaan met ICT-uitval.	· Inspectie van de afhankelijkheids analyse tussen zorg en ICT of uitgevoerde BIV classificatie of uitvalscenario's in voldoende mate zijn meegenomen.					
			c) De organisatie beschikt over één of meer continuïteitsplannen die gebaseerd zijn op deze risicoanalyse en periodiek worden geëvalueerd. In deze plannen is expliciet rekening gehouden met uitval als gevolg van een cyber security incident (zoals DDOS- of ransomware-aanval). Wanneer de kwaliteit van zorg en/of patiëntveiligheid door deze uitval naar mening van de raad van bestuur van een instelling gevaar loopt, zijn plannen en maatregelen uitgewerkt (met name voor spoedeisende zorg waarbij uitstel een gezondheidsrisico inhoudt), bijvoorbeeld door verplaatsing van zorgverlening naar andere ziekenhuizen.	· Inspectie van continuïteitsplan(nen) en uitgewerkte scenario's. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen.					
			d) De organisatie heeft hierbij, rekening houdend met de BIV-classificatie, een maximaal toegelaten uitvalsduur (MUD) en een maximaal toelaatbaar gegevensverlies (MGV) gedefinieerd voor de informatievoorziening.	· Inspectie van de BIV-classificatie en/of registratie van bedrijfsmiddelen (CMDB). Zie A.8.1.1.					
			e) De organisatie heeft als onderdeel van de continuïteitsplannen (nood)procedures en workarounds (zoals werken op papier) ontwikkeld en geïmplementeerd om in geval van ICT-verstoring en/of andere verstoringen de continuïteit van de (kritische) bedrijfsprocessen zo ver als mogelijk te handhaven en de oorza(a)k(en) van verstoring zo snel mogelijk weg te nemen.	· Inspectie van noodprocedures en workarounds als onderdeel van continuïteitsplan(nen).					
			f) De organisatie zorgt ervoor dat een crisisorganisatie is gedefinieerd en medewerkers met kennis van vitaal belang altijd bereikbaar zijn in geval van een calamiteit.	· Inspectie van de crisisorganisatie en actualiteit bereikbaarheidsinformatie					
			g) Bij ernstige ICT-uitval voert de organisatie een evaluatie uit, waarbij ook de (verhoogde kans op) schade voor zowel de patiënten in het ziekenhuis als eventueel voor de uitgeweken patiënten wordt geanalyseerd. Betrek in laatstgenoemde situatie ook partners in de zorgketen bij de evaluatie.	· Indien van toepassing inspectie van de evaluatie van een ICT incident met ernstige impact op de beschikbaarheid van ICT. · Interview met de verantwoordelijk functionaris(sen) over de evaluatie.					
			h) De organisatie beschikt over beleid, richtlijnen en procedures om in geval van een grootschalige crisis zoals een pandemie – dus vanuit bedrijfscontinuïteitbeheer – tijdelijke aanpassingen door te voeren in de ICT, teneinde de bestrijding van de crisis te kunnen ondersteunen. De aanpassingen zijn tijdelijk van aard en dienen na afloop van de crisis weer teruggedraaid te worden naar de oorspronkelijke situatie. Aanvullend vindt monitoring plaats in hoeverre de aanpassingen tot ongewenste nevenrisico's leiden en waar nodig wordt hierop geacteerd.	· Inspectie van beleid, richtlijnen en procedures om in geval van een grootschalige crisis tijdelijke maatregelen te treffen en na afloop deze weer te herstellen.					
	A.17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	Beheersmaatregel (bron: NEN 7510-1 annex A) De organisatie moet de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie test periodiek de doeltreffendheid van de technische en organisatorische maatregelen, de werking van de calamiteitenprocedures en de effectiviteit van de crisis- en continuïteitsplannen.	· Inspectie van het beleid, richtlijnen en procedures voor continuïteitswaarborging. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van ingerichte maatregelen. Zie voor best practice aanbevelingen het onderzoeksrapport van de OvV.					
			b) De organisatie test periodiek (minimaal jaarlijks) de continuïteitsmaatregelen van ICT-systemen in samenhang om te borgen dat de kritische zorgprocessen onder alle omstandigheden blijven functioneren. Ook dient geoefend te worden met scenario's waarbij de ICT in het ziekenhuis uitvalt zoals een cyber security aanval. Betrek afhankelijk van het te testen scenario externe partijen, zoals Regionaal Overleg Acute Zorgketen (ROAZ), collega-zorginstellingen en leveranciers bij deze oefeningen en testen.	· Inspectie van uitgevoerde continuïteitstesten van systemen/processen. · Interview met de verantwoordelijk functionaris(sen) over de resultaten van testen.					
			c) De organisatie neemt zo nodig aanvullende technische en organisatorische maatregelen, stelt waar nodig de calamiteitenprocedures en de crisis- en continuïteitsplannen bij.	· Inspectie van de evaluatie van uitgevoerde continuïteitstesten van systemen/processen. · Interview met de verantwoordelijk functionaris(sen) over het lerende vermogen.					
cryptografie	A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	Beheersmaatregel (bron: NEN 7510-1 annex A) Ter bescherming van informatie moet een beleid voor het gebruik van cryptografische beheersmaatregelen worden ontwikkeld en geïmplementeerd. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie heeft een encryptiebeleid vastgesteld. Dit beleid geeft invulling aan rollen, taken en verantwoordelijkheden, afdekking van relevante wet- en regelgeving, bewaartermijnen, sterkte en kwaliteit van het vereiste versleuteligsalgoritme, bescherming van sleutels (zie sleutelbeheer), impact van versleuteling op de controle van de inhoud (malware) en specifieke omstandigheden die uit risicoanalyses blijken.	· Inspectie van het beleid voor encryptie. · Interview met de verantwoordelijk functionaris(sen) over de opzet/het bestaan van het beleid. · Deelwaarneming op de juiste toepassing van het vastgestelde beleid.					
	A.10.1.2 Sleutelbeheer	Beheersmaatregel (bron: NEN 7510-1 annex A) Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels moet tijdens hun gehele levenscyclus een beleid worden ontwikkeld en geïmplementeerd. Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A) Geen.	a) De organisatie beschikt voor alle binnen de organisatie gebruikte versleuteltechnieken over procedures voor het beheren van cryptografische sleutels tijdens hun gehele levenscyclus met inbegrip van het aanmaken, bewaren, archiveren, terugvinden, distribueren, terugtrekken en vernietigen van sleutels	· Inspectie van procedures voor beheer van cryptografische sleutels. · Deelwaarneming(en) op de juiste toepassing van procedures voor het beheer van cryptografische sleutels.					
			b) De organisatie behoort alle cryptografische sleutels te beschermen tegen onbevoegd gebruik en apparatuur die wordt gebruikt om sleutels aan te maken, op te slaan en te archiveren behoort fysiek te worden beschermd.	· Inspectie van de logische en fysieke toegangsbeveiliging van systemen voor het beheren van cryptografische sleutels.					
			c) In de afweging van encryptie algoritmes en sleutelsterktes voor de versleuteling van persoonlijke gezondheidsinformatie past de organisatie 'best practices' toe.	· Ga na of toegepaste encryptiealgoritmes en sleutelsterktes voor bijvoorbeeld de inrichting van VPN, dataopslag, SSL verbindingen, etc aan het beleid en de best practices voldoen.					