Nederlandse Vereniging van Ziekenhuizen

Gedragslijn toegangsbeveiliging digitale patiëntdossiers 2.0

Deze gedragslijn is gericht op de onderdelen:

- Authenticatie
- Autorisatie
- Controle van logging
- Bewustwording van medewerkers op het gebied van informatiebeveiliging
- Beheer van bedrijfsmiddelen
- Cyber Security
- Leveranciersmanagement
- Beheer van informatiebeveiligingsincidenten
- Continuïteitsbeheer
- Cryptografie

Datum: 04-07-2022

Versie: 2.0

INHOUDSOPGAVE

1. INLEIDING

ACHTERGROND

Zorginstellingen, waaronder ziekenhuizen, zijn erop gericht om goede zorg te leveren aan de patiënten. Ter ondersteuning van het leveren van deze zorg gebruiken ziekenhuizen informatiesystemen en medische apparatuur, waarin persoonsgegevens inclusief persoonlijke gezondheidsinformatie worden vastgelegd (verder digitale patiëntdossiers). Het gebruik van deze systemen zorgt er onder andere voor dat informatie snel beschikbaar is binnen de organisatie en in samenhang kan worden gepresenteerd, waarmee goede patiëntenzorg en efficiëntie wordt bevorderd. Daarmee hebben beschikbaarheid, integriteit en vertrouwelijkheid van deze informatie invloed op de patiëntveiligheid.

Zorgverleners en ziekenhuizen hebben de verantwoordelijkheid om de persoonsgegevens van patiënten op een zorgvuldige wijze te registreren en invulling te geven aan het medisch beroepsgeheim. Met de invoering van de Algemene Verordening Gegevensbescherming (verder AVG) kent de Europese Unie één wet die de bescherming van persoonsgegevens regelt. In Nederland is het verwerken van persoonsgegevens betreffende de gezondheid tevens geregeld in de Uitvoeringswet AVG en is het medisch beroepsgeheim verankerd in de Wet op de Geneeskundige Behandelingsovereenkomst (verder WGBO) en de Wet op de Beroepen in de Individuele Gezondheidszorg (verder Wet BIG). WGBO en Wet BIG dienen ter bescherming van (persoons)gegevens en het gebruik ervan in de zorg.

Organisatorische en technische maatregelen moeten onrechtmatige en onnodige verwerking van en toegang tot persoonsgegevens voorkomen, waarbij er blijvende aandacht is voor patiëntveiligheid. Het inrichten van een adequaat niveau van informatiebeveiliging is hiervoor noodzakelijk.

Reeds in de Regeling gebruik Burgerservicenummer in de zorg van 26 mei 2008 en de AMvB Elektronische gegevensverwerking door zorgaanbieders van 10 november 2017 is het voldoen aan NEN7510 (alsmede NEN7512 en NEN7513) als randvoorwaarde gesteld voor het verwerken van persoonlijke gezondheidsinformatie van patiënten en elektronische gegevensverwerking van deze informatie door en tussen zorgaanbieders. Er is dus geen sprake van nieuwe verplichtingen.

CONCRETE GEDRAGSLIJN NOODZAKELIJK

De NVZ en de NFU willen duidelijkheid bieden nu de Autoriteit Persoonsgegevens (verder AP) eisen van informatiebeveiliging in de zorg volgens NEN 7510 heeft gehanteerd in haar toezicht. In de norm NEN 7510 is voor een aantal eisen de praktische uitwerking niet of onvoldoende nader gespecificeerd. Hierbij ontbreekt consensus over wat een passende mate van informatiebeveiliging is, ook met inachtneming van andere voorwaarden zoals de stand der techniek en patiëntveiligheid. Om tot een ‘best practice’ voor ziekenhuizen te komen, hebben de NVZ en de NFU in eerste instantie in oktober 2020 versie 1.0 en nu deze uitgebreidere gedragslijn 2.0 ontwikkeld.

DOELSTELLING

Deze gedragslijn heeft tot doel de ziekenhuizen te ondersteunen bij de praktische implementatie van de normeisen rondom privacy en informatiebeveiliging van digitale patiëntdossiers (persoonlijke gezondheidsinformatie) op basis van NEN 7510.

UITGANGSPUNTEN

In gedragslijn 1.0 was het uitgangspunt dat de zorginstelling beschikt over een Managementsysteem voor informatiebeveiliging (oftewel: Information Security Management System, hierna: ISMS), zoals beschreven in NEN 7510-1. Dit bleek in de praktijk nog niet voor alle instellingen het geval te zijn. NEN 7510 schrijft voor dat een instelling over een ISMS dient te beschikken. De gedragslijn en het bijbehorende toetsingskader bieden ondersteuning bij de invulling daarvan.

De gedragslijn kan gebruikt worden om de maatregelen in het ISMS nader in te vullen. Beoogde beveiligingsmaatregelen moeten, met als uitgangspunt de geldende wet- en regelgeving, tot stand komen op basis van een risicoanalyse. Het uitgangspunt is dat de maatregelen passend moeten zijn, ook vanuit een kosten-/baten-afweging.

GEDRAGSLIJN EN TOETSINGSKADER

Deze gedragslijn voor ziekenhuizen richt zich op de privacy en informatiebeveiliging rondom de toegang tot persoonlijke gezondheidsinformatie. In versie 1.0 van de gedragslijn zijn de maatregelen nader uitgewerkt voor de volgende aandachtsgebieden die door de AP als cruciaal zijn aangegeven:

- Authenticatie
- Autorisaties
- Logging en controle van logging
- Bewustwording van medewerkers op het gebied van informatiebeveiliging

In versie 2.0 van de gedragslijn zijn aanvullende gebieden uit NEN 7510 uitgewerkt, waarvan een werkgroep bestaande uit de NVZ en 8 ziekenhuizen heeft bepaald dat deze een hoog risico kennen en/of nadere duiding behoeven:

- Beheer van bedrijfsmiddelen
- Cyber Security (feitelijk een samenvoeging van meer onderdelen)
- Leveranciersmanagement
- Beheer van informatiebeveiligingsincidenten
- Continuïteitsbeheer
- Cryptografie

Om de implementatie van de gedragslijn te ondersteunen, is een toetsingskader opgesteld waarin meer achtergrondinformatie en een testaanpak is opgenomen.

NORMERING

Binnen deze gedragslijn gelden per aandachtsgebied beheersmaatregelen en zorgspecifieke beheersmaatregelen, die rechtstreeks afkomstig zijn uit NEN 7510:2017 deel 1, inclusief Annex A, uitgewerkt in deel 2. In NEN 7510:2017 deel 1

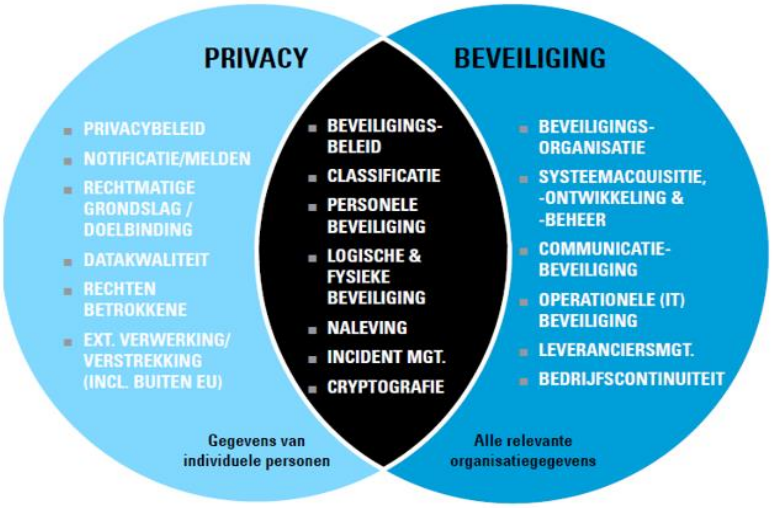
staat dat zorginstellingen de beheersmaatregelen selecteren op basis van de risicoanalyse en het van toepassing zijn vastleggen in de verklaring van toepasselijkheid.

Per beheersmaatregel zijn een aantal criteria opgenomen. Deze dienen als handreiking voor een zorginstelling om aan de beheersmaatregel te voldoen.

2. RELATIE PRIVACY EN INFORMATIEBEVEILIGING

Informatiebeveiliging speelt een belangrijke rol in het privacybeschermings-vraagstuk. Zo hebben informatiebeveiliging en privacybescherming een duidelijk gemeenschappelijk doel, namelijk de bescherming van waardevolle en gevoelige bedrijfsinformatie. Daarbinnen biedt informatiebeveiliging de noodzakelijke en concrete maatregelen die nodig zijn om bescherming van vertrouwelijke informatie te kunnen realiseren.

De relatie tussen privacy en informatiebeveiliging wordt weergegeven in Figuur 1[1]. De onderwerpen in de cirkel 'beveiliging' komen overeen met de hoofdstukken van NEN 7510-1 annex A.



Figuur 1 - relatie privacy en informatiebeveiliging

De verwerkingsverantwoordelijke (in de regel de Directie van de zorginstelling) hoort passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Zorgaanbieders moeten invulling geven aan de verplichting door toepassing van de NEN-normen voor informatiebeveiliging in de gezondheidszorg (NEN 7510, 7512 en 7513).

Voor een volledige afdekking van de relevante informatiebeveiligingsonderwerpen in het kader van privacy zijn ten minste alle NEN 7510-onderwerpen in de overlap tussen privacy en informatiebeveiliging relevant. Om te voldoen aan NEN 7510 zijn alle onderwerpen in de cirkel 'beveiliging' van belang.

NEN 7510-1 vereist verder dat een zorginstelling relevante maatregelen selecteert uit NEN 7510-1 annex A op basis van de risicoanalyse en deze vastlegt in de verklaring van toepasselijkheid en daarmee kan aantonen dat de maatregelen wel of niet van toepassing zijn. De zorginstelling borgt op basis van een Plan-Do-Check-Act-cyclus (verder PDCA-cyclus) dat aan de NEN 7510-norm wordt voldaan.

[1] Bron figuur: de IT-Auditor - Naar een volwassen privacy-implementatie d.d. 8 september 2017

Passende beveiliging is daarbij altijd gerelateerd aan de actuele stand van de techniek, de uitvoeringskosten, alsook de aard, de omvang, de context en het doel van de gegevensverwerking (zie artikel 32 EU-AVG). Het is nodig om in de organisatie als onderdeel van het ISMS een PDCA-cyclus in te richten voor de periodieke evaluatie van de beveiligingsmaatregelen, waaronder ook de toegang tot patiëntgegevens behoort.

In de volgende hoofdstukken, die reeds waren uitgewerkt in de Gedragslijn 1.0, zijn de volgende onderwerpen uitgewerkt:

- Autorisaties en Authenticatie (hoofdstuk 4)
- Logging en controle van logging en (hoofdstuk 5)
- Bewustwording medewerkers (hoofdstuk 6)

Gedragslijn 1.0 ging ervan uit dat een instelling over een ISMS beschikte. Hoofdstuk 3 van Gedragslijn 2.0, 'Managementsysteem voor informatiebeveiliging (ISMS)' en het bijbehorende toetsingskader bieden ondersteuning bij de invulling daarvan.

Gedragslijn 2.0 geeft daarnaast een aanvullende uitwerking van de NEN 7510-onderwerpen, waarvan de ziekenhuizen uit de NVZ-werkgroep 'Gedragslijn 2.0' hebben bepaald dat deze een hoog risico kennen en/of nadere duiding behoeven:

- Beheer van bedrijfsmiddelen (hoofdstuk 7);
- Cyber Security (hoofdstuk 8);
- Leveranciersmanagement (hoofdstuk 9);
- Beheer van informatiebeveiligingsincidenten (hoofdstuk 10);
- Continuïteitsbeheer (hoofdstuk 11)
- Cryptografie (hoofdstuk 12).

Deze Gedragslijn 2.0 vervangt integraal de Gedragslijn 1.0.

3. MANAGEMENTSYSTEEM VOOR INFORMATIEBEVEILIGING (ISMS)

INLEIDING

Wet- en regelgeving schrijft voor dat de instelling dient te voldoen aan NEN 7510 en derhalve dient te beschikken over een ISMS conform de richtlijnen en definities van NEN 7510-1. De Gedragslijn 2.0 sluit aan bij NEN 7510-1 voor de specifieke vereisten die hieraan worden gesteld. In het toetsingskader is ter verduidelijking een testaanpak uitgewerkt voor het uitvoeren van een self-assessment.

ALGEMEEN

NEN 7510 voor informatiebeveiliging in de zorg bestaat uit twee delen. NEN 7510-1 is opgesteld om te voorzien in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van het Managementsysteem voor informatiebeveiliging (ISMS).

NEN 7510-2 voorziet in nadere richtlijnen voor de invulling van de beheersmaatregelen in NEN 7510-1 annex A over hoe men het beste de beschikbaarheid, integriteit en vertrouwelijkheid van dergelijke informatie kan beschermen. In NEN 7510-2 staan 'best practices' of richtlijnen om aan de NEN 7510-1 te voldoen. Dit zijn mogelijke keuzes, daarom worden in NEN 7510-2 de beheersmaatregelen niet normatief beschreven; er staat dus geen 'moeten', maar 'behoren te'. Zorginstellingen moeten deze beheersmaatregelen selecteren op basis van de risicoanalyse en deze vastleggen in de verklaring van toepasselijkheid en kunnen daarmee aantonen dat de beheersmaatregelen wel of niet van toepassing zijn.

TOEPASSINGSGEBIED

De verplichtingen uit de NEN 7510-norm zijn van toepassing op alle verwerkingen van de persoonsgegevens van patiënten. Omdat gegevensuitwisseling tussen zorgaanbieders in toenemende mate elektronisch plaatsvindt, heeft deze norm ook betrekking op de gegevensuitwisseling tussen aanbieders van gezondheidszorg.

Zorginstellingen worden aangeraden door middel van een risicoanalyse zelf een gelaagdheid aan te brengen om het toepassingsgebied (scope) van het ISMS te bepalen. In die risicoanalyse dient ook aandacht te zijn voor e-Health toepassingen en bijvoorbeeld de rol van een afdeling klinische fysica & medische technologie (voor zover aanwezig). Zie hiervoor ook het Convenant Medische Technologie. Van belang is dat de zorginstelling de risico's inzichtelijk heeft die gepaard gaan met het koppelen van apparatuur aan zorginformatiesystemen en uitwisselingssystemen voor persoonlijke gezondheidsinformatie.

VEREISTEN EN TOETSINGSKADER ISMS

Het ISMS is een managementsysteem dat op basis van een beoordeling van bedrijfsrisico's tot doel heeft het vaststellen, implementeren, uitvoeren, controleren,

beoordelen, onderhouden en verbeteren van informatiebeveiliging. Deze activiteiten worden periodiek herhaald.

Het managementsysteem voor informatiebeveiliging borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door een risicobeheerproces toe te passen en geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerst. Dit betekent concreet dat zorginstellingen:

1. risicobeoordelingen van informatiebeveiliging met geplande tussenpozen uitvoeren, of als significante veranderingen worden voorgesteld of zich voordoen;
2. het behandelplan van informatiebeveiligingsrisico's opstellen en implementeren en alle beheersmaatregelen vaststellen die nodig zijn om de informatiebeveiligingsrisico's tot een acceptabel niveau te reduceren;
3. beheersmaatregelen naar behoefte ontwerpen en vergelijken met die in bijlage A van NEN 7510-1 om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten.

Voor meer informatie omtrent NEN 7510 zie de NEN-standaarden die vrijelijk beschikbaar zijn. In NEN 7510-2:2017 Bijlage B is een praktisch plan van aanpak opgenomen voor het implementeren van NEN 7510-1.

4. CRITERIA AUTORISATIES EN AUTHENTICATIE

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A voor het aandachtsgebied autorisaties en authenticatie zijn in dit hoofdstuk weergegeven. In het bij deze Gedragslijn behorende toetsingskader is een nadere toelichting met onderbouwing opgenomen.

A.9.1.1 BELEID VOOR TOEGANGSBEVEILIGING

Beheersmaatregel (bron: NEN 7510-1 annex A)
Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 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 cliënt-gerelateerde 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.

Criteria gedragslijn
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.

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.
c) Gebruikers en dienstverleners behoren een duidelijke instructie te ontvangen waarin is vastgelegd aan welke bedrijfseisen de toegangsbeveiligings-maatregelen moeten voldoen.
d) De organisatie heeft richtlijnen voor toegang middels noodprocedures.
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[2] hebben uitsluitend toegang tot persoonlijke gezondheidsinformatie indien zij een behandelrelatie[3] 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.

[2] Onder medewerker wordt tevens verstaan externe zorgverlener, medewerker van externe leverancier, contractant, vrijwilliger, onderzoeker en student indien relevant voor het onderwerp.

[3] Voor de definitie van behandelrelatie wordt verwezen naar de richtlijn van KNMG - Omgaan met medische gegevens d.d.15 april 2021. Daarin staat opgenomen dat rechtstreeks betrokkenen in het algemeen personen zijn die als team, op gelijkgerichte wijze, betrokken zijn bij het doel waarvoor de gegevens worden verstrekt. Te denken valt aan personen die de arts bij zijn werkzaamheden assisteren, zoals verpleegkundigen, doktersassistenten en diëtisten. Maar onder de rechtstreeks betrokkenen valt ook de collega-vakgenoot aan wie advies wordt gevraagd in het kader van de behandeling.

A.9.2.1 REGISTRATIE EN AFMELDEN VAN GEBRUIKERS

Beheersmaatregel (bron: NEN 7510-1 annex A)

Een formele registratie- en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 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.

Criteria gedragslijn
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.
b) De organisatie hanteert bij de uitdiensttreding en/of het beëindigen van de opdracht procedures voor het intrekken van toegangsrechten en -bevoegdheden.
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.
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.
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.

A.9.2.2 GEBRUIKERS TOEGANG VERLENEN

Beheersmaatregel (bron: NEN 7510-1 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 7510-1 annex A)
Geen.

Criteria gedragslijn
a) De organisatie heeft in een autorisatiematrix aangegeven welke soorten informatie voor welke functies van medewerkers voor de uitvoering van hun werk noodzakelijk zijn.
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.
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.
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.

A.9.2.3 BEHEREN VAN SPECIALE TOEGANGSRECHTEN

Beheersmaatregel (bron: NEN 7510-1 annex A)
Het toewijzen en gebruik van speciale toegangsrechten moet worden beperkt en beheerst.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A)
Geen.

Criteria gedragslijn
a) De organisatie heeft procedures om ten behoeve van het functioneel en technisch beheer van systemen aan beheerders speciale bevoegdheden toe te kennen.
b) De betrokken medewerkers zijn bevoegd en bekwaam voor de uitvoering van de specifieke taken.
c) Uitvoering van de specifieke taken en het gebruik van de speciale bevoegdheden worden gelogd.
d) Het verantwoordelijk management ziet toe op de naleving en blokkeert de bevoegdheden (tijdelijk) wanneer gebruik niet (langer) noodzakelijk is.

A.9.2.5 BEOORDELING VAN TOEGANGSRECHTEN VAN GEBRUIKERS

Beheersmaatregel (bron: NEN 7510-1 annex A)
Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A)
Geen.

Criteria gedragslijn
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.

A.9.2.6 TOEGANGSRECHTEN INTREKKEN OF AANPASSEN

Beheersmaatregel (bron: NEN 7510-1 annex A)
De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten moeten bij beëindiging van hun dienstverband, contract of overeenkomst worden verwijderd en bij wijzigingen moeten deze worden aangepast.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 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.

Criteria gedragslijn
a) De organisatie heeft een procedure met betrekking tot het intrekken/aanpassen van logische toegangsrechten.
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.
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.
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.

A.9.4.1 BEPERKING TOEGANG TOT INFORMATIE

Beheersmaatregel (bron: NEN 7510-1 annex A)
Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A)
Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het

verwerken van persoonlijke gezondheidsinformatie moet geïsoleerd (en gescheiden) worden van de toegang tot de informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.

Criteria gedragslijn

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.
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.
c) De organisatie hanteert op het interne netwerk een MFA door middel van minimaal twee verschillende factoren[4], 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

[4] Kortom: MFA is in- en extern de standaard. Tenzij er een gegronde reden (stand der techniek, patiëntveiligheid, infectiepreventie, etc.) is om hiervan af te wijken. Dit is in een risicoanalyse verder uitgewerkt en door het management vastgesteld en goedgekeurd. Vanuit de risicoanalyse zijn alternatieve maatregelen beschreven en ingericht om een passend beheersingsniveau te bereiken, zoals automatische vergrendeling (schermbeveiliging), EPD-sessie time-out, fysieke toegangsbeveiliging, etc.

Onder MFA (Multi Factor Authenticatie) verstaat de Gedragslijn een authenticatiemethode waarbij de gebruiker toegang krijgt nadat met succes twee of meer factoren zijn voorgelegd aan een authenticatiemechanisme, die verschillen in kennis, bezit en/of overerving. Het netwerk (zonering, gelaagdheid) wordt niet als authenticatiefactor gezien.

bij vermissing van de token de medewerker hier onmiddellijk melding van maakt, waarna de token direct (tijdelijk) wordt geblokkeerd[5].

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.

A.9.4.3 SYSTEEM VOOR WACHTWOORDBEHEER

Beheersmaatregel (bron: NEN 7510-1 annex A)
Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A)
Geen.

Criteria gedragslijn
De organisatie zorgt dat vereiste wachtwoordconventies door systeeminstellingen worden ondersteund en afgedwongen.

[5] Gracing is niet standaard toegestaan, dit is een afwijking op het MFA-beleid. Hiervoor geldt zoals beschreven in hoger liggende bullit, dat er een gegronde reden (stand der techniek, patiëntveiligheid, infectiepreventie, etc.) moet zijn om af te wijken van MFA. Dit is in een risicoanalyse verder uitgewerkt en door het management vastgesteld en goedgekeurd. Vanuit de risicoanalyse zijn alternatieve maatregelen ingericht om een passend beheersingsniveau te bereiken.

5. CRITERIA LOGGING EN CONTROLE OP LOGGING

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A en NEN 7513 voor het aandachtsgebied logging en controle op logging zijn in dit hoofdstuk weergegeven. In het bij deze gedragslijn behorende toetsingskader is een nadere toelichting met onderbouwing opgenomen.

A.12.4.1 GEBEURTENISSEN REGISTREREN

Beheersmaatregel (bron: NEN 7510-1 annex A)
Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, minimaal vijf jaar worden bewaard en regelmatig worden beoordeeld.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A)
Geen.

Criteria gedragslijn

a) De organisatie maakt het door middel van logging mogelijk achteraf onweerlegbaar vast te stellen welke gebeurtenissen hebben plaatsgevonden op een digitaal patiëntdossier.
b) De bewaartermijn voor logging is minimaal vijf (5) jaar (60 maanden) of zo lang als het dossier wordt bewaard[6].
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.
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.

[6] Zie voor meer achtergrondinformatie - Besluit van de Minister voor Medische Zorg van 27 juni 2019, kenmerk 1529221-190512-WJZ, houdende vaststelling van een bewaartermijn voor logging.

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[7]:
   - welke gebeurtenis heeft plaatsgevonden;
   - datum en tijdstip van de gebeurtenis;
   - welke cliënt het betrof;
   - wie de gebruiker was.

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.

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.

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.

[7] In NEN 7513:2018 zijn voor specifieke doelgroepen aanvullende eisen beschreven t.a.v. logging. Deze zijn niet in de Gedragslijn opgenomen.

A.12.4.2 BESCHERMEN VAN INFORMATIE IN LOGBESTANDEN

Beheersmaatregel (bron: NEN 7510-1 annex A)
Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 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.

Criteria gedragslijn
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.

6. CRITERIA BEWUSTWORDING MEDEWERKERS

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A voor het aandachtsgebied 'Bewustwording medewerkers' zijn in dit hoofdstuk weergegeven. In het bij deze gedragslijn behorende toetsingskader is een nadere toelichting met onderbouwing opgenomen.

A.7.2.2 BEWUSTZIJN, OPLEIDING EN TRAINING TEN AANZIEN VAN INFORMATIEBEVEILIGING

Beheersmaatregel (bron: NEN 7510-1 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 7510-1 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, aan 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.

Criteria gedragslijn
a) Een bewustzijnsprogramma is opgesteld dat structureel geplande, periodiek geactualiseerde bewustwordingsactiviteiten bevat.
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).
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.
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.

e) Om de kennisoverdracht en de gedragsverandering te meten (en daarmee de effectiviteit van het bewustzijnsprogramma) wordt deelname aan het bewustzijnsprogramma gemeten en vinden analyses plaats op de trendmatige ontwikkeling van gemelde informatiebeveiligingsincidenten.

7. CRITERIA BEHEER VAN BEDRIJFSMIDDELEN

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A voor het aandachtsgebied 'Beheer van bedrijfsmiddelen' zijn in dit hoofdstuk weergegeven.

Doelstelling is dat bedrijfsmiddelen van de organisatie zijn geïdentificeerd en passende verantwoordelijkheden ter bescherming zijn gedefinieerd.

Het hebben van een sluitende assetregistratie (CMDB) is een belangrijke randvoorwaarde voor informatiebeveiliging en privacy. Als er bijvoorbeeld een beveiligingslek is gerapporteerd, dan kan door middel van analyse van het CMDB bepaald worden waar zich het lek (potentieel) kan voordoen, zodat hierop gerichte vervolgacties plaatsvinden.

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.

Criteria gedragslijn
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.
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.
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.
d) De organisatie zorgt dat de classificatie en inventarisatie actueel zijn.
e) De organisatie beschikt over regels voor het aanvaardbare gebruik van deze bedrijfsmiddelen.
f) De organisatie zorgt voor een juiste gang van zaken als het bedrijfsmiddel wordt verwijderd of vernietigd.

8. CRITERIA CYBER SECURITY

ALGEMEEN

Het aantal dreigingen uit de hoek van Cyber Security neemt steeds meer toe. Dit vraagt om passende maatregelen. Tegenwoordig is het niet meer voldoende om de bedrijfsmiddelen die persoonlijke gezondheidsinformatie bevatten alleen met preventieve maatregelen te beschermen. Organisaties moeten ervan uitgaan dat ze ieder moment gehackt kunnen zijn. Organisaties dienen weerbaar te zijn om bij aanvallen, incidenten en/of calamiteiten deze adequaat te detecteren en hierop snel te reageren. Deze weerbaarheid noemt men wel 'Cyber Resilience'.

In dit hoofdstuk is een aantal maatregelen uit NEN 7510-1 annex A geselecteerd die bijdragen aan het verbeteren van Cyber Security en Cyber Resilience. Deze inventarisatie is niet volledig en bevat alleen die maatregelen die een hoog risico kunnen mitigeren en/of nadere duiding behoeven. De maatregelen dienen door ieder ziekenhuis aangevuld te worden met de maatregelen die als onderdeel van het risicobehandelproces zijn geselecteerd om geïdentificeerde risico's verder te mitigeren.

De geselecteerde maatregelen hebben betrekking op de volgende onderwerpen:

- Telewerken
- Bescherming tegen malware
- Beheer van technische kwetsbaarheden
- Scheiding in netwerken
- Technische beoordeling van toepassingen na wijzigingen
- Leveranciersmanagement (zie hoofdstuk 9)
- Beheer van informatiebeveiligingsincidenten (zie hoofdstuk 10)
- Continuïteit (zie hoofdstuk 11)

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.

Criteria gedragslijn

a) De organisatie heeft richtlijnen en procedures voor telewerken opgesteld en geïmplementeerd[8]. 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

[8] Zie https://www.ncsc.nl/onderwerpen/veilig-thuiswerken voor actuele voorbeelden en standaarden op het gebied van veilig thuiswerken.

van meekijken en meeluisteren huisgenoten) en het verantwoord virtueel samenwerken.
b) De organisatie hanteert voor externe toegang tot systemen die persoonlijke gezondheidsinformatie bevatten passende beveiligde (versleutelde) verbindingen en MFA.
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.
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.

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.

Criteria gedragslijn
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).
b) De organisatie houdt de beschermingsmaatregelen up-to-date conform de nieuwste definities en inzichten en logt detectie en verwijdering van kwaadaardige software.
c) De organisatie evalueert periodiek de werking van de beschermingsmaatregelen.
d) De organisatie herstelt waar nodig de negatieve gevolgen van kwaadaardige software en andere inbreuken.
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.

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.

Criteria gedragslijn
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.
b) De organisatie heeft een proces ingericht om tijdig alerts te ontvangen. De ontvangen alerts worden geëvalueerd en indien nodig tijdig opgevolgd.
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.).
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.

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.

Criteria gedragslijn
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.
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

c) De organisatie beschikt over beleid waarin is vastgelegd welke uitgangspunten voor segmentering zijn gehanteerd en welke koppelvlakken zijn ingericht.
d) Alle gescheiden groepen hebben een beveiligingsniveau dat refereert aan de classificatie en het beleid van de organisatie.
e) Van informatiesystemen en servers wordt bijgehouden in welk segment ze staan. Dit overzicht dient actueel te zijn.

A.14.2.3 TECHNISCHE BEOORDELING VAN TOEPASSINGEN NA WIJZIGINGEN BESTURINGSPLATFORM

Beheersmaatregel (bron: NEN 7510-1 annex A)
Als besturingsplatforms zijn veranderd, moeten bedrijfskritische toepassingen worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A)
Geen.

Criteria gedragslijn
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.
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.
c) Als het beleid inzake pentesten of de uitgevoerde risicoanalyse daartoe aanleiding geeft, voert de organisatie een penetratietest uit (zie A.18.2.3).

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.

Criteria gedragslijn
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[9];
- 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.

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.

[9] Zie NOREA Handreiking bij DigiD-assessments V2.0, d.d. 19 december 2016 en NOREA Update van de testaanpak DigiD-assessment 2.0, d.d. 26 mei 2020 voor nadere achtergrondinformatie hieromtrent.

9. CRITERIA LEVERANCIERSMANAGEMENT

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A voor het aandachtsgebied 'Leveranciersmanagement' zijn in dit hoofdstuk weergegeven.

NEN 7510 beoogt met leveranciersmanagement de volgende doelstellingen te bereiken:

- Het waarborgen van de bescherming van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers;
- Het handhaven van een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten.

In het bij deze gedragslijn behorende toetsingskader is een nadere toelichting met onderbouwing opgenomen.

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-infrastructuur-elementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.

Zorgspecifieke beheersmaatregel (bron: NEN 7510-1 annex A)
Geen.

Criteria gedragslijn

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.).
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.
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).

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).
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[10]. 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.

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.

Criteria gedragslijn
a) De organisatie controleert en beoordeelt periodiek de dienstverlening door externe partijen.
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).
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.

[10] Specifieke vereisten voor de aanschaf en het gebruik van e-Health toepassingen en Medische Technologie zijn beschreven in het toetsingskader IGJ 'Inzet van e-Health door zorgaanbieders' respectievelijk 'Convenant Veilige Toepassing van Medische Technologie in de medisch specialistische zorg' en de Medical Device Regulation (MDR).

10. CRITERIA BEHEER VAN INFORMATIEBEVEILIGINGSINCIDENTEN

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A voor het aandachtsgebied 'Incident management' zijn in dit hoofdstuk weergegeven.

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

In het bij deze gedragslijn behorende toetsingskader is een nadere toelichting met onderbouwing opgenomen.

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. om een doeltreffende en tijdige respons op informatiebeveiligingsincidenten te bewerkstelligen;
2. om te garanderen dat er een doeltreffend en geprioriteerd escalatiepad is voor incidenten zodat in de juiste omstandigheden en tijdig een beroep kan worden gedaan op plannen voor crisismanagement en bedrijfscontinuïteitsmanagement;
3. om 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.

Criteria gedragslijn

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.

b) De organisatie heeft procedures voor het melden en classificeren van informatiebeveiligingsincidenten.
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.
d) De organisatie hanteert een procedure voor het indien noodzakelijk informeren van de patiënt en eventuele toezichthouders.

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.

Criteria gedragslijn
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.
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.

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.

Criteria gedragslijn
a) Periodieke effectevaluatie vindt plaats om combinaties van verschillende incidenten en/of terugkerende of ingrijpende incidenten te identificeren.

b) De effectiviteit van bestaande risicoanalyses en beheersmaatregelen wordt op basis van de analyse geëvalueerd, waar nodig bijgesteld en aan het verantwoordelijk management gerapporteerd.
c) De organisatie gebruikt waar relevant de uitkomsten van de uitgevoerde evaluaties om het informatieveiligheidsbewustzijn van medewerkers te bevorderen.

11. CRITERIA CONTINUÏTEITSBEHEER

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A voor het aandachtsgebied 'Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer' zijn in dit hoofdstuk weergegeven.

Doelstelling is dat informatiebeveiligingscontinuïteit moet zijn ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

NEN 7510 hanteert de term informatiebeveiligingscontinuïteit. Hierbij gaat het om de continuïteit van de processen en informatievoorziening die van belang zijn voor de verlening van zorg.

In het bij deze gedragslijn behorende toetsingskader is een nadere toelichting met onderbouwing opgenomen.

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.

Criteria gedragslijn

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).
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.
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.
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.
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.

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.
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.
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.

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.

Criteria gedragslijn

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.
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.
c) De organisatie neemt zo nodig aanvullende technische en organisatorische maatregelen, stelt waar nodig de calamiteitenprocedures en de crisis- en continuïteitsplannen bij.

12. CRITERIA CRYPTOGRAFIE

ALGEMEEN

De relevante beheersmaatregelen uit NEN 7510-1 annex A voor het aandachtsgebied 'Cryptografie' zijn in dit hoofdstuk weergegeven.

Doelstelling is het zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

In het bij deze gedragslijn behorende toetsingskader is een nadere toelichting met onderbouwing opgenomen.

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.

Criteria gedragslijn
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 versleutelingsalgoritme, bescherming van sleutels (zie sleutelbeheer), impact van versleuteling op de controle van de inhoud (malware) en specifieke omstandigheden die uit risicoanalyses blijken.[11]

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.

Criteria gedragslijn
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.

[11] Zie https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging voor actuele voorbeelden en standaarden op het gebied van versleuteling van verbindingen.

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.
c) In de afweging van encryptie algoritmes en sleutelsterktes voor de versleuteling van persoonlijke gezondheidsinformatie past de organisatie 'best practices' toe.

BIJLAGE 1: ACHTERGROND WETGEVING EN BEGRIPPEN

In diverse wetten en besluiten (AMVB's), zoals onder andere de AVG, WGBO, Wet BIG en het Besluit elektronische gegevensverwerking door zorgaanbieders, zijn bepalingen opgenomen over het verwerken van persoonsgegevens van patiënten. Deze wetten en besluiten regelen door wie, voor welke doeleinden en onder welke voorwaarden persoonsgegevens mogen worden verwerkt en aan anderen mogen worden verstrekt. In deze bijlage is een aantal voor dit onderwerp relevante wetten en besluiten verkort weergegeven. Meer informatie is te vinden op de website website: https://www.nen.nl/nen-7510-1-2017-a1-2020-nl-267179.

Deze gedragslijn is aanvullend op huidige of toekomstige, wettelijke of in de regelgeving bepaalde vereisten.

ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG)

Deze privacywetgeving is sinds 2018 in de gehele Europese Unie van toepassing. De AVG geeft het wettelijk kader aan voor het verwerken van persoonsgegevens, zoals gezondheidsgegevens en stelt eisen hoe hiermee om te gaan. De Nederlandse implementatie van de AVG is vastgelegd in de Uitvoeringswet AVG (UAVG).

DE WET OP DE GENEESKUNDIGE BEHANDELINGSOVEREENKOMST (WGBO)

De WGBO ligt aan de basis van de zorgverlening. In de WGBO staan de rechten en plichten beschreven van zorgverleners en patiënten die zorg krijgen. De WGBO regelt de dossierverplichting van de hulpverlener en verankert de geheimhoudingsplicht in de behandelrelatie.

WET OP DE BEROEPEN IN DE INDIVIDUELE GEZONDHEIDSZORG (BIG)

Het doel van de Wet BIG is te zorgen dat de kwaliteit van onze gezondheidszorg hoog is en blijft. Ook beschermt de Wet BIG patiënten tegen ondeskundig en onzorgvuldig handelen van zorgverleners. Dit doet de Wet BIG onder andere met het BIG-register. Ook is in de Wet BIG het beroepsgeheim van professionals opgenomen en verankerd in het tuchtrecht.

VAN TOEPASSING ZIJNDE BEGRIPPEN

De in deze gedragscode gehanteerde begrippen zijn direct afgeleid van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg 2020 (Wabvpz) voorheen de 'Gedragscode EGiZ, Elektronische gegevensuitwisseling in de zorg' (KNMG, Nictiz, september 2019). Een aantal in deze wet gehanteerde begrippen uit de hiervoor genoemde gedragscode hebben wij hierna weergegeven.

a) AP: de Autoriteit Persoonsgegevens als bedoeld in artikel 6 Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG);
b) AVG: Algemene Verordening Gegevensbescherming;
c) Behandelrelatie: de relatie tussen de Betrokkene en de Zorgaanbieder met wie de cliënt een behandelingsovereenkomst als bedoeld in artikel 7:446, eerste lid WGBO heeft, of degene die rechtstreeks betrokken is bij de uitvoering van die

behandelingsovereenkomst, of degene die optreedt als vervanger van degene die een behandelingsovereenkomst heeft met de cliënt;

d) Behandelingsovereenkomst: de overeenkomst bedoeld in artikel 7:446 lid 1 WGBO waarbij een natuurlijke persoon of een rechtspersoon, de hulpverlener, zich in de uitoefening van een geneeskundig beroep of bedrijf tegenover een ander, de opdrachtgever, verbindt tot het verrichten van handelingen op het gebied van de geneeskunst, rechtstreeks betrekking hebbende op de persoon van de opdrachtgever of van een bepaalde derde;
e) Logging: elektronische vastlegging van acties met betrekking tot het gebruik van een Elektronisch Uitwisselingssysteem en/of een zorginformatiesysteem;
f) Persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
g) WGBO: Wet geneeskundige behandelingsovereenkomst, zoals opgenomen in Boek 7, Titel 7, Afdeling 5 van het Burgerlijk Wetboek;

BIJLAGE 2: RELEVANTE NEN - NORMEN VOOR DE GEDRAGSLIJN

Het gebruik van de NEN 7510-, 7512- en 7513-normen vanuit een compliance-gedachte brengt een aantal belangrijke overwegingen met zich mee.

NEN 7510

NEN 7510 voor informatiebeveiliging in de zorg bestaat uit twee delen. Deel 1 is opgesteld om te voorzien in eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van het Managementsysteem voor informatiebeveiliging (ISMS). Het ISMS is dat deel van een managementsysteem dat op basis van een beoordeling van bedrijfsrisico's tot doel heeft het vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en verbeteren van informatiebeveiliging.

Het managementsysteem voor informatiebeveiliging borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door een risicobeheerproces toe te passen en geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerst. Dit betekent concreet dat zorginstellingen:

1. risicobeoordelingen van informatiebeveiliging met geplande tussenpozen uitvoeren, of als significante veranderingen worden voorgesteld of zich voordoen;
2. het behandelplan van informatiebeveiligingsrisico's opstellen en implementeren en alle beheersmaatregelen vaststellen die nodig zijn om de informatiebeveiligingsrisico's tot een acceptabel niveau te reduceren;
3. beheersmaatregelen naar behoefte ontwerpen en vergelijken met die in bijlage A van NEN 7510-1 om te verifiëren dat geen noodzakelijke beheersmaatregelen zijn weggelaten.

NEN 7510-2 voorziet in nadere richtlijnen voor de invulling van de beheersmaat-regelen in NEN 7510-1 annex A over hoe men het beste de beschikbaarheid, integriteit en vertrouwelijkheid van dergelijke informatie kan beschermen. In NEN 7510-2 staan 'best practices' of richtlijnen om aan NEN 7510-1 te voldoen. Dit zijn mogelijke keuzes, daarom worden in NEN 7510-2 de beheersmaatregelen niet normatief beschreven; er staat dus geen 'moeten', maar 'behoren te'. Zorginstellingen moeten deze beheersmaatregelen selecteren op basis van de risicoanalyse en deze vastleggen in de verklaring van toepasselijkheid en kunnen daarmee aantonen dat de beheersmaatregelen wel of niet van toepassing zijn. Deel 1 is het equivalent van ISO-27001, deel 2 het equivalent van ISO-27002, in beide gevallen met zorgspecifieke aanvullingen. Partijen zoals leveranciers buiten de zorg zullen zich veelal richten op de ISO-normen.

RELATIE MET NEN 7512 EN NEN 7513

NEN 7512 en 7513 geven een nadere invulling aan beheersmaatregelen uit NEN 7510. Binnen de zorg worden gegevens in toenemende mate uitgewisseld tussen betrokken partijen. Dit geldt voor zowel de primaire processen van behandeling en verzorging van een individuele patiënt als voor de financiële afhandeling en de bedrijfsprocessen in een zorginstelling. NEN 7512 heeft betrekking op (het maken van

afspraken over) de elektronische communicatie in de zorg, en wel tussen zorgverleners en zorginstellingen onderling, met patiënten en cliënten, met zorgverzekeraars en met andere partijen die bij de zorg zijn betrokken. NEN 7512 beschrijft het proces om te komen tot een goede risicobeoordeling voor gegevensuitwisseling.

NEN 7513 stelt eisen aan de registratie van gegevens rondom de toegang tot elektronisch vastgelegde persoonlijke gezondheidsinformatie bij een zorginstelling of een andere organisatie die persoonlijke gezondheidsinformatie verwerkt. NEN 7513 beschrijft de gebeurtenissen die moeten worden gelogd en welke gegevens van die gebeurtenissen moeten worden vastgelegd.

BIJLAGE 3: CONTROLE VAN TOEGANG TOT PATIËNTDOSSIERS

Een zorginstelling heeft richtlijnen voor toegang tot patiëntdossiers zowel voor reguliere toegang als toegang middels noodprocedures. Deze gebruikers-activiteiten worden geregistreerd in logbestanden. Zorginstellingen controleren deze logbestanden. De controle van logging richt zich minimaal op de logresultaten van de noodprocedure ('breaking the glass'-procedure) en toegang tot patiëntdossiers.

De logging vindt bij voorkeur plaats door middel van geautomatiseerde of integrale controle. De controle van logging kan ook plaatsvinden door middel van deelwaarneming en steekproef. Hiervoor kunnen ook geautomatiseerde hulpmiddelen worden ingezet.

Indien de autorisaties zo zijn ingericht dat deze borgen dat toegang tot het patiëntdossier alleen mogelijk is voor personen die hiertoe bevoegd zijn en anders de noodprocedure in werking treedt, volstaat het om alleen de logging van de noodprocedure te controleren.

Controle van de logging de noodprocedure
De controle van de logging van het gebruik van de noodprocedure is een procesgerichte controle. Vastgesteld wordt of de noodprocedure terecht is uitgevoerd. De noodprocedure is een gedefinieerd proces. Voor het toetsen van een proces is een procesgerichte controle d.m.v. deelwaarneming de vaktechnische norm. Indien de noodprocedure door middel van deelwaarneming wordt gecontroleerd, dient het aantal te controleren gebeurtenissen op jaarbasis minimaal 60 te zijn. Bij het selecteren van deelwaarnemingen zoekt de organisatie gericht naar gebeurtenissen met een verhoogd risico, zoals VIP's, interessante ziektebeelden of collega's die zijn opgenomen in het ziekenhuis.

Bij het bepalen van dit aantal is gebruik gemaakt van de steekproefaanpak die ook door accountants bij hun controlewerkzaamheden wordt gehanteerd zoals beschreven in de SRA-praktijkhandreiking 'Systeemgerichte controlewerk-zaamheden', d.d. 5 maart 2018. Uitgegaan is van hoog risico gebeurtenissen (ongeautoriseerde inzage patiëntdossiers en AVG-compliance risico) die meerdere keren per dag plaatsvinden, zie tabel 1. Indien noodprocedures minder vaak plaatsvinden, kan het aantal waarnemingen hierop worden aangepast.

Frequentie gebeurtenis	Aantal deelwaarnemingen per jaar		
	Hoog risico	Medium risico	Laag risico
Jaar	1	1	1
Kwartaal	2	2	2
Maand	5	4	2
Week	15	10	5
Dag	40	30	20
Meerdere keren per dag	60	45	25

Tabel 1 - bepalen aantal deelwaarnemingen procesgerichte controle[12]

[12] Bron: SRA-praktijkhandreiking 'Systeemgerichte controlewerkzaamheden', 5 maart 2018

Controle van de logging van toegang tot patiëntdossier
Controle van de logging van toegang tot patiëntdossiers is een gegevensgerichte controle. Vastgesteld wordt of het patiëntdossier terecht is ingezien. Indien deze controle door middel van een steekproef wordt uitgevoerd, dient het aantal te controleren gebeurtenissen op jaarbasis minimaal 60 te zijn. Hierbij hoeft niet verder beoordeeld te worden dan de gebeurtenissen van het afgelopen jaar.

Bij het bepalen van dit aantal is gebruik gemaakt van de steekproefaanpak die ook door accountants bij hun controlewerkzaamheden wordt gehanteerd, zoals beschreven is in de SRA–Praktijkhandreiking 'Gegevensgerichte Steekproeven/ model SRA Steekproefmethode', d.d. 1 juli 2019. Zie daarnaast voor nadere toelichting https://www.deitauditor.nl/wp-content/uploads/2014/09/artikel-7-statische-steekproef.pdf voor meer achtergrondinformatie.

In geval van een statistische steekproef op een homogene massa en een 0-fouten hypothese is de steekproefomvang, ongeacht de omvang van de zorginstelling, het aantal patiëntdossiers en het aantal inzagen, minimaal 60 patiëntdossiers op jaarbasis.

Uitgangspunt hierbij is dat het een homogene massa betreft. Het minimaal aantal van 60 is gebaseerd op de volgende formule:

Steekproefomvang = R-factor / Nauwkeurigheid = 3 / 0,05 = 60

R-Factor is 3,00, zie bijgevoegde tabel, gebaseerd op een betrouwbaarheidseis van 95% en een verwachte fout van nul. De nauwkeurigheid (toelaatbare fout) is 5%.

Betrouwbaarheidseis in %	**R-Factoren**			
Verwachte fout	*Nul*	*Een*	*Twee*	*Drie*
99	4,61	6,64	8,41	10,05
95	**3,00**	4,75	6,30	7,76
90	2,31	3,89	5,33	6,69
85	1,90	3,38	4,73	6,02
80	1,61	3,00	4,28	5,52
75	1,39	2,70	3,93	5,11

Tabel 2 - R-factoren bij verschillende betrouwbaarheidseisen

De 0 verwachte fouten hypothese hanteert men als men op voorhand uitgaat geen afwijkingen te constateren in de steekproef. Indien wel afwijkingen verwacht worden (bijvoorbeeld omdat de awareness nog laag is bij medewerkers), is het beter een hogere fouten hypothese te hanteren. De steekproefomvang neemt dan toe. Bij een 3-fouten hypothese, 95% betrouwbaarheid en 5% nauwkeurigheid bedraagt de omvang 7,76 / 0,05 = 156 (afgerond).

Uitgangspunt van de steekproefaanpak is dat de fijnmazigheid van het gehanteerde autorisatiemodel en de controle op de juistheid van de autorisaties mede bepalend zijn voor de intensiteit van de controle op de logging. Het minimumaantal van 60 patiëntdossiers op jaarbasis is gebaseerd op een

autorisatiemodel dat voldoet aan de definitie van behandelrelatie in de Gedragslijn.

Daar waar de organisatie ervoor kiest hiervan af te wijken, voert de instelling een risicoanalyse uit en treft passende alternatieve beheersmaatregelen. Passende beheersmaatregelen zijn bijvoorbeeld het periodiek uitvoeren van aanvullende controles (geautomatiseerd en/of gerichte deelwaarneming) bovenop de steekproefomvang om te borgen dat er een systematiek is geïmplementeerd, waarmee het risico op onrechtmatig gebruik van autorisaties om persoonlijke gezondheidsinformatie in te zien tijdig kan worden gedetecteerd en gecorrigeerd.

BIJLAGE 4: TERMEN EN DEFINITIES

Voor de toepassing van deze gedragslijn gelden de volgende termen en definities.

actie: verwerking in een informatiesysteem, in het kader van een gebeurtenis

assetregister: een assetregister of CMDB (Configuration Management Database) is een hulpmiddel voor het bijhouden van alle benodigde informatie over de applicaties die bij een organisatie in beheer zijn

audit: systematisch, onafhankelijk en gedocumenteerd proces voor het verkrijgen van auditbewijsmateriaal en het objectief beoordelen daarvan om vast te stellen in welke mate aan de criteria is voldaan

authenticatie: het verschaffen van zekerheid met betrekking tot de juistheid van een geclaimde karakteristiek

autorisatie: toekennen van bevoegdheden

bedrijfsmiddel: alles wat waarde heeft voor de organisatie, bijvoorbeeld een informatiesysteem, Medische Technologie, apparaten/e-Health toepassingen, etc.

beheersmaatregel: elke vorm van proces, beleid, voorziening, werkwijze of andere maatregel waarmee het risico wordt gewijzigd

beleid: intenties en richting van een organisatie zoals formeel door verantwoordelijk management kenbaar gemaakt

beoordeling: activiteit die wordt ondernomen om de geschiktheid, toereikendheid en doeltreffendheid van het desbetreffende onderwerp voor het behalen van vastgestelde doelstellingen te bepalen

beschikbaarheid: eigenschap van het toegankelijk en bruikbaar zijn op verzoek van een bevoegde entiteit

breaking the glass: het bewust buiten de zorgrelatie om verkrijgen van toegang tot patiëntgegevens in noodgevallen (patiëntveiligheid). Het systeem genereert een melding aan de gebruiker en logt de betreffende gebeurtenis.

cliënt (patiënt): persoon die zorg vraagt of aan wie zorg wordt verleend of de identificeerbare persoon van wie persoonlijke gezondheidsinformatie wordt verwerkt

cliëntgegevens: medische, verpleegkundige, sociale en administratieve gegevens betreffende individuele cliënten

directie: persoon of groep van personen die een organisatie op het hoogste niveau bestuurt en beheert

dienstverband: relatie van een persoon met een organisatie voor het uitvoeren van bepaalde taken door die persoon

e-Health: de inzet van hedendaagse informatie- en communicatietechnologie in de zorg om de zorg te ondersteunen en/of te verbeteren. Ook de term ‘digitale zorg’

wordt hier wel voor gebruikt. Voorbeelden zijn patiëntenportalen, medische apps en monitoring van chronische patiënten op afstand.

endpoint protection: beveiligt apparaten, zoals mobiele apparaten, laptops, desktop-pc's van eindgebruikers en servers en zorgt ervoor dat externe devices, die een connectie met het interne netwerk willen maken, voldoen aan de geldende beveiligingsrichtlijnen (policies)

gebeurtenis: optreden van of wijziging in een bepaalde combinatie van omstandigheden

gebruiker: natuurlijke persoon, organisatie of proces in een informatiesysteem, betrokken bij een actie

governance: systeem van geleiding en beheersing

gracing: de mogelijkheid bieden om een gebruikerssessie 'mee te nemen' naar een andere werkplek door middel van het aanbieden van een strikt individuele/persoonlijke token (bijvoorbeeld een medewerkerspas)

identificatie: bepalen van de identiteit van een persoon of andere entiteit

identificator: kenmerk dat een persoon of andere entiteit identificeert

informatiebeveiliging: behoud van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie

informatiebeveiligingsgebeurtenis: het zich voordoen en waargenomen worden van een systeem-, dienst- of netwerksituatie die op een mogelijke schending van het informatiebeveiligingsbeleid of falen van beheersmaatregelen wijst, of van een voorheen onbekende situatie die mogelijk relevant is voor de beveiliging

informatiebeveiligingsincident: afzonderlijke gebeurtenis of een reeks informatiebeveiligingsgebeurtenissen waarvan het zeer waarschijnlijk is dat deze de bedrijfsactiviteiten compromitteren en de informatiebeveiliging in gevaar brengen

informatiedomein: gespecificeerd gebied waarbinnen de verantwoordelijkheden voor de informatievoorziening zijn bepaald, dezelfde regels gelden voor informatiebeveiliging en dezelfde systematiek wordt gevolgd voor identificatie van personen, systemen en andere objecten

informatiesysteem: toepassingen, diensten, informatietechnologische bedrijfsmiddelen of andere gegevensverwerkende componenten

Information Security Management System (ISMS): zie managementsysteem voor informatiebeveiliging

integriteit: eigenschap van nauwkeurigheid en volledigheid

Intrustion Detection System (IDS): een geautomatiseerd systeem dat ongeautoriseerde toegang tot een informatiesysteem of netwerk detecteert

Intrusion Prevention System (IPS): een beveiligingsapparaat dat gebruikt wordt om het netwerkverkeer te monitoren op ongewenst gedrag en deze te blokkeren

loggen: voorvallen, activiteiten of het optreden van wijzigingen in een informatiesysteem chronologisch vastleggen

logging: resultaat van het loggen

managementsysteem: geheel van samenhangende of elkaar beïnvloedende elementen van een organisatie om een beleid en doelstellingen vast te stellen, alsmede de processen om die doelstellingen te bereiken

managementsysteem voor informatiebeveiliging (ISMS): dat deel van een managementsysteem dat op basis van een beoordeling van bedrijfsrisico's tot doel heeft het vaststellen, implementeren, uitvoeren, controleren, beoordelen, onderhouden en verbeteren van informatiebeveiliging

medewerker: personeel in loondienst en personeel niet in loondienst, hieronder wordt ook verstaan externe zorgverlener, medewerkers van externe leverancier, contractant, vrijwilliger, onderzoeker en student indien relevant voor het onderwerp

medische apparatuur: apparatuur die wordt gebruikt als hulpmiddel voor een zorgproces en waarop persoonlijke gezondheidsinformatie wordt verwerkt

MFA (Multi Factor Authenticatie): authenticatiemethode waarbij de gebruiker pas toegang krijgt nadat met succes twee of meer factoren zijn voorgelegd aan een authenticatiemechanisme die verschillen in kennis, bezit en overerving

noodprocedure: in de context van de Gedragslijn wordt onder noodprocedure de 'breaking the glass'-procedure verstaan

object: zaak of persoon waarop een actie betrekking heeft

organisatie: persoon of groep van personen die zijn eigen functies heeft met verantwoordelijkheden, bevoegdheden en relaties om zijn doelstellingen te bereiken

patiëntdossier: de vastgelegde patiëntgegevens die worden verzameld in het kader van de verleende zorg

persoonlijke gezondheidsinformatie: informatie over een identificeerbare persoon die verband houdt met de lichamelijke of geestelijke gesteldheid van, of de verlening van zorgdiensten aan, de persoon in kwestie, waaronder ook begrepen kan worden:

a) informatie over de registratie van de persoon voor de verlening van zorgdiensten;

b) informatie over betalingen of het in aanmerking komen voor zorg met betrekking tot de persoon;

c) een aan een persoon toegewezen nummer, symbool of bijzonderheid als unieke identificatie van die persoon voor medische doeleinden;

d) alle informatie over de persoon die wordt vergaard tijdens het verlenen van zorgdiensten aan de persoon;

e) informatie die is ontleend aan een beproeving of onderzoek van een lichaamsdeel of lichaamseigen stof, en

f) identificatie van een persoon (bijvoorbeeld een zorgprofessional) als verlener van zorg aan de persoon.

richtlijn: beschrijving die verduidelijkt wat behoort te worden gedaan en hoe, om de doelstellingen te bereiken die in het beleid zijn vastgelegd

risico: effect van onzekerheid op het behalen van doelstellingen

risicoanalyse: proces dat tot doel heeft de aard van het risico te begrijpen en het risiconiveau vast te stellen

risicobeoordeling: gehele proces van risico-identificatie, risicoanalyse en risico-evaluatie

Security Operations Center (SOC): bedoeld om beveiligingsproblemen in IT-systemen en IT-infrastructuur te voorkomen, op te sporen, te beoordelen en erop te reageren

toegangsbeveiliging: middel om te bewerkstelligen dat toegang tot bedrijfsmiddelen wordt goedgekeurd en beperkt op basis van de eisen voor bedrijfsvoering en beveiliging

Third party mededeling (TPM): mededeling (rapport) van een onafhankelijke auditor over de opzet, het bestaan en/of de werking van het stelsel van beveiligingsmaatregelen van een organisatie ten behoeve van de klanten van die organisatie. Door Amerikaanse invloeden is ook wel de term SOC-rapportage in gebruik: Service Organisation Control rapportage)

verantwoordelijke management: degene die het beleid opstelt, beslissingen neemt en consequenties draagt ten aanzien van een organisatie, een object of de inhoud en uitvoering van een proces

verantwoordelijke gebruiker: natuurlijke persoon die verantwoordelijk is voor een actie

verificatie: bevestiging dat aan gespecificeerde eisen is voldaan door het verschaffen van objectief bewijs

verklaring van toepasselijkheid: gedocumenteerde verklaring die de beheersdoelstellingen en beheersmaatregelen beschrijft die relevant en toepasbaar zijn op het managementsysteem voor informatiebeveiliging van de organisatie

vertrouwelijkheid: eigenschap dat informatie niet beschikbaar of niet bekend wordt gemaakt aan onbevoegde personen, entiteiten of processen

verwerking: een bewerking of geheel van bewerkingen van persoonsgegevens of geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens

Vulnerabilty scanning: testen op bekende kwestbaarheden zoals het nog niet geïnstalleerd zijn van de laatste beveiligingsupdates op een server; dit gebeurt bij voorkeur met geautomatiseerde hulpmiddelen; deze hulpmiddelen kunnen steeds

meer (zoals automatisch patchen) en vertonen bij inzet van AI steeds meer overlap met andere hulpmiddelen (IDS/IPS/SIEM)

whitelisting: een whitelist is een lijst die regelt wat is toegestaan, bijvoorbeeld een lijst met toegestane applicaties/apps of een lijst met IP-adressen of servers die als vertrouwd worden beschouwd en waarvan verbindingen of berichten zijn toegestaan wanneer alles standaard wordt geweigerd.

zorg: zorg als omschreven in de Wet langdurige zorg en de Zorgverzekeringswet en alle andere verrichtingen, inclusief het onderzoeken en het geven van raad, die rechtstreeks betrekking hebben op een persoon en ertoe strekken diens gezondheid te bevorderen of te bewaken

zorgaanbieder: zorgverlener of zorginstelling

zorginformatiesysteem: informatiesysteem ter ondersteuning van een zorgverlener

zorginstelling: rechtspersoon die bedrijfsmatig zorg verleent, alsmede een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen, alsmede een natuurlijke persoon die bedrijfsmatig zorg doet verlenen, alsmede een solistisch werkende zorgverlener

zorgverlener: een natuurlijke persoon die beroepsmatig zorg verleent