Nederlandse Vereniging van Ziekenhuizen

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Handreiking
Assurance-opdracht Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0

Handreiking voor de IT-auditor bij het uitvoeren van een assurance-opdracht om de vermelding van het management omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 te controleren.

Versie 1.0
26 februari 2021

Inhoudsopgave

Hyperlinks volgen zodra publieke NVZ webpagina beschikbaar is!

1 Gedragslijn toegangsbeveiliging 1.0 assurance-opdracht

1.1 Aanleiding

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 waarin de digitale persoonlijke gezondheidsinformatie van patiënten worden vastgelegd (verder patiëntdossiers). Het gebruik van informatiesystemen zorgt er onder andere voor dat informatie snel beschikbaar is binnen de organisatie waar dat nodig is, informatie in samenhang kan worden gepresenteerd 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 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 medisch beroepsgeheim verankerd in de Wet op de Geneeskundige Behandelovereenkomst (verder WGBO) en de Wet op de Beroepen in de Individuele Gezondheidszorg (verder BIG). WGBO en 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 goede autorisatie door zorginstellingen, en het daarmee hanteren van de juiste identificatie en authenticatie, is noodzakelijk.

De Autoriteit Persoonsgegevens heeft in haar toezicht in de zorg beheersingsmaatregelen[1] uit NEN 7510 annex A gehanteerd. In de norm NEN 7510 is de praktische uitwerking niet of onvoldoende nader gespecificeerd. Elke zorginstelling is nu in zekere mate vrij om deze eisen te interpreteren. 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 te komen, hebben de NVZ en de NFU als onderdeel van de routekaart de gedragslijn 'toegangsbeveiliging digitale patiëntdossiers versie 1.0' (hierna: de Gedragslijn) ontwikkeld. De Gedragslijn is in oktober 2020 door de besturen van de NVZ en NFU vastgesteld en goedgekeurd. In nauwe samenhang met de Gedragslijn hebben de NVZ/NFU het auditkader 'Gedragslijn toegangsbeveiliging digitale patiëntdossiers versie 1.0' (hierna: het Auditkader) opgesteld en gepubliceerd.

De NVZ heeft begin 2020 een routekaart vastgesteld. Onderdeel van de routekaart is dat ziekenhuizen aantoonbaar voldoen aan de vereisten in de Gedragslijn. Hiervoor dienen ziekenhuizen een 0-meting en een 1-meting door middel van een assurance-opdracht uit te voeren. Ziekenhuizen voeren de 0-meting uit door middel van self-assessment. Als basis hiervoor dient het Auditkader. Daarnaast heeft de NVZ een template-rapport opgesteld, waarin de resultaten van de 0-meting worden vastgelegd. Dit rapport met als bijlage het ingevulde auditkader, is door de zorginstelling op uiterlijk 11 januari 2021 naar de NVZ verzonden. Nadat ziekenhuizen de gaps uit de 0-meting hebben opgevolgd, dient uiterlijk in mei 2021 een assurance-opdracht ten behoeve van de 1-meting (hierna: assurance-opdracht) te worden uitgevoerd. De assurance-opdracht dient door een Register IT-auditor (RE) uitgevoerd te worden, door middel van de Nederlandse Richtlijn 3000A 'Assurance-opdrachten door IT-auditors (Attest-opdrachten)' vastgesteld door de Nederlandse Orde van Register EDP-auditors (NOREA), hierna genoemd: richtlijn 3000A. De NVZ zal op basis hiervan een geanonimiseerd en geaggregeerd rapport van de 1-meting samenstellen, waarin op hoofdlijnen de status wordt beschreven van de implementatie van de Gedragslijn onder haar leden. Het geaggregeerde rapport is bedoeld voor het bestuur van de NVZ en verantwoording aan de toezichthouder (AP).

[1] Met de term beheersingsmaatregel wordt in deze handreiking hetzelfde bedoeld als een beheersmaatregel, zoals in NEN7510 en de Gedragslijn zijn beschreven.

1.2 Doel handreiking

Doelstelling van deze handreiking is de betrokken IT-auditors een uniform kader te bieden voor het zorgvuldig uitvoeren van de assurance-opdracht om de vermelding van het management omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 te controleren. Voorkomen moet worden dat er grote verschillen ontstaan in de mate van diepgang bij uitvoering van de assurance-opdrachten als bij het vaststellen van afwijkingen. Waar mogelijk/ wenselijk moet ook duidelijk zijn wat minimaal c.q. maximaal gedaan zou moeten worden om tot redelijke mate van zekerheid te komen. Het is daarom uitdrukkelijk niet de bedoeling voor de assurance-opdracht aanvullende normen van NEN7510 af te leiden. Dit doet niet af aan de opvatting van de NVZ dat organisaties er goed aan doen om op basis van een risicoanalyse te bepalen welke overige NEN7510 maatregelen geïmplementeerd moeten worden om zodoende de beschikbaarheid, integriteit en vertrouwelijkheid van informatiesystemen te borgen.

De handreiking geeft een leidraad voor het uitvoeren van de assurance-opdracht. Het blijft echter de professionele verantwoordelijkheid van de IT-auditor om op basis van een deugdelijke grondslag tot een oordeel te komen. De richtlijn 3000A van de NOREA is daarbij leidend. Bij verschillen van inzicht is het primair aan de betrokken IT-auditors om in overleg tot een oplossing te komen. De NVZ kan daarbij eventueel als gesprekspartner deelnemen.

1.3 Doelstelling Gedragslijn ‘toegangsbeveiliging digitale patiëntdossiers’

De Gedragslijn heeft tot doel de zorginstellingen te ondersteunen bij de praktische implementatie van de normeisen rondom toegangsbeveiliging van digitale patiëntdossiers. De gedragslijn richt zich op de ziekenhuis brede informatiesystemen.

De Nederlandse Vereniging van Ziekenhuizen (NVZ) en de Nederlandse Federatie van Universitair Medische Centra (NFU) hebben in oktober 2020 aan hun leden versie 1.0 van de ‘Gedragslijn toegangsbeveiliging digitale patiëntdossiers’ (hierna: de Gedragslijn) beschikbaar gesteld. De Gedragslijn richt zich op de toegang tot de digitale patiëntdossiers. De Gedragslijn geeft de doelstellingen en de beheersingsmaatregelen weer van de volgende aandachtsgebieden:

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

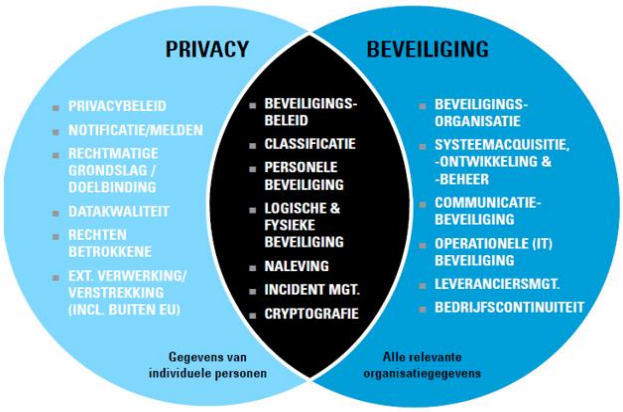
Om de implementatie van de gedragslijn te ondersteunen, is een auditkader opgesteld, waarin meer achtergrondinformatie en een testaanpak is opgenomen.

De Gedragslijn is in oktober 2020 vastgesteld door de besturen van de NVZ en de NFU.

1.4 Achtergrond Gedragslijn ‘toegangsbeveiliging digitale patiëntdossiers’

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. 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 (RvB 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).

Binnen de Gedragslijn gelden per aandachtsgebied beheersingsmaatregelen en zorgspecifieke beheersingsmaatregelen, die rechtstreeks afkomstig zijn uit NEN 7510:2017 deel 1 – Annex A. Deze beheersingsmaatregelen dienen beschouwd te worden als norm c.q. de te bereiken doelstellingen. Zie Tabel 2 in hoofdstuk 2 voor een overzicht van de beheersingsmaatregelen in scope van de Gedragslijn. In NEN 7510:2017 deel 1 staat dat zorginstellingen de beheersingsmaatregelen selecteren op basis van de risicoanalyse en het van toepassing zijn vastleggen in de verklaring van toepasselijkheid. Voor de beheersingsmaatregelen die in de Gedragslijn zijn opgenomen, geldt dat deze altijd van toepassing zijn.

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.

Per beheersingsmaatregel zijn in het auditkader een aantal toetsingscriteria opgenomen. Deze dienen als handreiking voor een zorginstelling om aan de beheersingsmaatregel te voldoen.

Daar waar de zorginstelling gegronde redenen heeft (stand der techniek, patiëntveiligheid, infectiepreventie, etc.) om af te wijken van de toetsingscriteria, dient de zorginstelling dit in een risicoanalyse uit te werken, die door management is vastgesteld en goedgekeurd. Vanuit de risicoanalyse dienen alternatieve maatregelen te zijn ingericht om een passend beheersingsniveau te bereiken. De IT-auditor neemt indien van toepassing kennis van de uitgevoerde risicoanalyses en stelt vast dat deze zijn gedocumenteerd en door het management zijn goedgekeurd.

Uitgangspunt van de Gedragslijn is dat de zorginstelling beschikt over een managementsysteem voor informatiebeveiliging (Information Security Management System, verder ISMS), zoals beschreven in NEN 7510-1. De gedragslijn dient geïntegreerd te zijn in het ISMS binnen de zorginstelling. Beoogde beveiligingsmaatregelen moeten tot stand komen op basis van een risicoanalyse. Het uitgangspunt moet zijn dat de maatregelen passend zijn, ook vanuit een kosten-/baten-afweging. Het ISMS maakt geen onderdeel uit van het object van onderzoek.

2 Formele aspecten van het onderzoek

De assurance-opdracht inzake het controleren van de vermelding van het management omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 wordt door RE's uitgevoerd overeenkomstig Richtlijn 3000A. Voor het assurance-rapport is een modelrapport opgesteld dat door de IT-auditor moet worden gehanteerd voor de assurance-opdracht. Daarnaast gelden tevens de Richtlijnen voor kwaliteitsbeheersing, opdrachtaanvaarding en documentatie, zoals die van toepassing zijn voor alle professionele diensten die door RE's worden uitgevoerd.

De werkzaamheden in het kader van deze opdracht richten zich op het geven van een oordeel met redelijke mate van zekerheid dat de vermelding van het management, in alle van materieel belang zijnde aspecten, een getrouw beeld geeft omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 op onderzoeksdatum. Indien afwijkende bevindingen daartoe aanleiding geven, geeft de IT-auditor deze weer in de paragraaf 'De basis voor ons [oordeel/ oordeel met beperking/ afkeurend oordeel/ oordeelsonthouding]'

Het rapport wordt uitsluitend verstrekt en gebruikt ten behoeve van de betreffende organisatie en de NVZ. De reden hiervoor is de vertrouwelijkheid en dat anderen, die niet op de hoogte zijn van de precieze scope, aard en doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

Indien wel voldaan is aan de opzet van de norm, maar het bestaan van beheersingsmaatregelen niet vastgesteld kon worden omdat de relevante gebeurtenis zich niet heeft voorgedaan in de onderzochte periode dan wordt dit weergegeven als "voldoet". In de bevinding wordt de volgende zin opgenomen: ''Wij hebben vastgesteld dat deze organisatie maatregelen heeft ontworpen en ingericht met betrekking tot deze norm en hebben deze gevalideerd. Vanwege het feit dat zich geen situatie heeft voorgedaan waarop deze maatregel betrekking heeft, hebben wij het bestaan niet kunnen vaststellen."

2.1 Object van onderzoek

De scope van onderzoek wordt enerzijds bepaald door de doelstellingen en bijbehorende beheersingsmaatregelen van de Gedragslijn en anderzijds op de systemen die vallen onder de definitie van het ziekenhuis brede informatiesysteem.

De scope van de Gedragslijn sluit niet uit dat er systemen en beheersingsmaatregelen binnen de zorginstelling zijn, die niet tot het object van onderzoek behoren van de Gedragslijn, maar wel risico's met zich mee kunnen brengen ten aanzien van privacy en security. Het blijft te allen tijde de verantwoordelijkheid van de zorginstelling om te voldoen aan wet- en regelgeving.

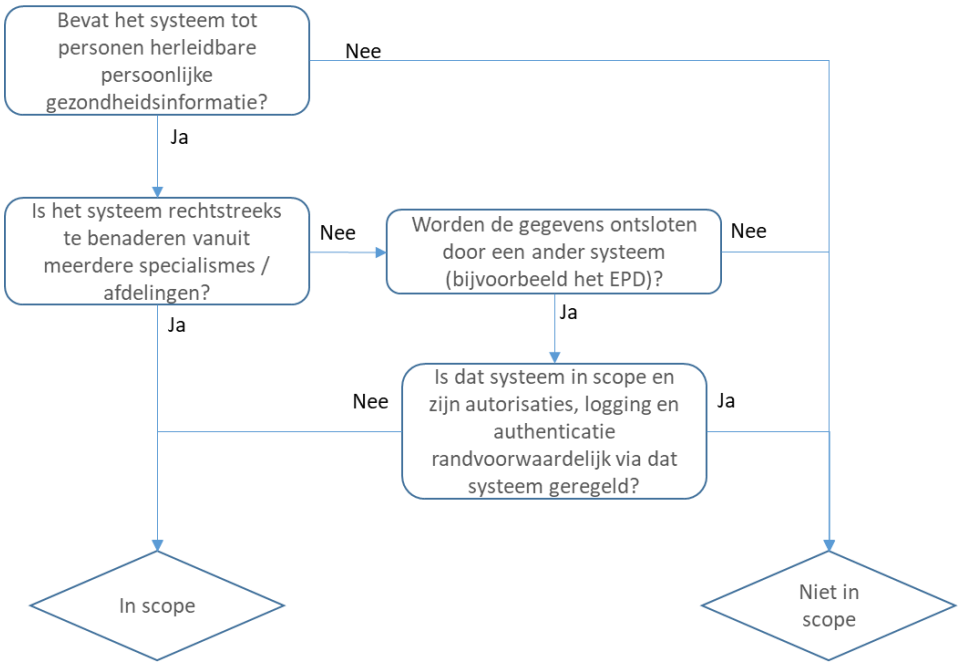
Scope Ziekenhuis breed Informatiesysteem

Onder Ziekenhuis breed Informatiesysteem verstaat de Gedragslijn systemen die tot personen herleidbare persoonlijke gezondheidsinformatie bevatten en benaderbaar zijn voor meerdere specialismes. Hieronder vallen minimaal het centrale Elektronische Patiënten Dossier (hierna: EPD), maar mogelijk ook één of meer van onderstaande systemen.

- een EPD specifiek voor functie of afdeling, waarin meerdere specialisme toegang hebben (bijvoorbeeld voor OK, Intensive care, moeder/kind, oogheelkunde of Dialyse). Benadrukt wordt dat bij samenwerkingsverbanden waar meerdere EPD's voorkomen, deze EPD's in scope zijn van de Gedragslijn indien deze vallen onder bovenstaande definitie van Ziekenhuisbreed Informatiesysteem.
- het Elektronisch Voorschrijf Systeem (hierna: EVS)
- Patiëntenportaal en/of zorgverlenersportaal
- Medische technologie waar meerdere specialisme toegang toe hebben waaronder lab (uitslag) systemen en Radiologie/beeld systemen.

- Een datawarehouse (mits hierin tot personen herleidbare persoonlijke gezondheidsinformatie geregistreerd is')
- Een acceptatie omgeving of andere kopie-omgeving van het EPD waarin niet geanonimiseerde persoonlijke gezondheidsinformatie is opgeslagen.

Hanteer onderstaande beslisboom om te bepalen of systemen onderdeel uitmaken van een ziekenhuis breed informatiesysteem, en daarmee onderdeel is van de scope van de assurance-opdracht. Leg het doorlopen van de beslisboom als evidence vast in het dossier behorende bij de assurance-opdracht.



Figuur 2 – beslisboom scope bepaling Ziekenhuisbreed Informatiesysteem

In veel hedendaagse EPD's worden specialistische systemen ontsloten of dagelijks geïnterfacet met het EPD. De gegevens kunnen vervolgens via het EPD door andere specialismes worden geraadpleegd, als dit noodzakelijk is voor de behandeling. Deze specialismes hebben geen rechtstreekse toegang tot het onderliggende specialistische systeem. Hiermee biedt het EPD (of het bovenliggende besturingssysteem) de randvoorwaardelijke borging van autorisaties, authenticatie en logging.

Indien dit het geval is, dan hoeft het specialistisch systeem niet in scope te zijn van de assurance-opdracht.

Voorbeeld scope bepaling door de zorginstelling:
De zorginstelling beschikt over een systeem ter ondersteuning van het Klinisch Chemisch Laboratorium. De uitslagen worden in een KCL systeem/ database vastgelegd, die ontsloten wordt via het EPD. Via het EPD hebben andere specialismes toegang tot de KCL uitslagen. Deze specialismes hebben niet rechtstreeks toegang tot het KCL systeem.

Valt KCL in scope van de Gedragslijn?

Allereerst gaat de zorginstelling na of de aandachtsgebieden/ beheersingsmaatregelen voor toegang tot de KCL uitslagen via het EPD worden geborgd. Bij de meest gangbare EPD's is dit het geval. Met andere woorden de autorisaties, logging en authenticatie worden randvoorwaardelijk via het EPD geborgd.

Aanvullend biedt het KCL systeem de mogelijkheid om rechtstreeks toegang te krijgen tot de gegevens. Het systeem bevat alle lab uitslagen die naar een persoon te herleiden zijn. Echter de achterliggende diagnostische gegevens zijn niet vastgelegd in het KCL systeem, deze bevinden zich in het EPD.

Daarnaast stelt de zorginstelling vast of de rechtstreekse toegang breder is dan de KCL afdeling. Indien de toegang beperkt is tot een aantal medewerkers van het laboratorium en deze medewerkers vanuit hun functie ook geautoriseerd zijn om deze gegevens te mogen raadplegen, valt het systeem niet onder de definitie van Ziekenhuis breed Informatiesysteem.

Figuur 3 – voorbeeld scope bepaling door zorginstelling

Scope beheersingsmaatregelen

De Gedragslijn heeft betrekking op de aandachtsgebieden (bewustwording, autorisaties, authenticatie en logging), risico's en de realisatie van deze aandachtsgebieden door middel van het inrichten van beheersingsmaatregelen. Deze beheersingsmaatregelen dienen beschouwd te worden als norm c.q. de te bereiken doelstellingen.

Aandachtsgebied	Inherente risico Gedragslijn 1.0	Realisatie aandachtsgebied door:
1. Bewustwording	Het risico dat medewerkers van de zorginstelling door onbewust handelen een privacy- of informatiebeveiligingsincident veroorzaken en hiermee schade toebrengen aan (het imago van) de zorginstelling.	Beheersingsmaatregelen gericht op het borgen dat medewerkers van de zorginstelling op het gebied van informatiebeveiliging een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie krijgen, voor zover relevant voor hun functie.
2. Autorisaties	Het risico dat medewerkers van de zorginstelling onbevoegd en zonder doelbinding tot personen herleidbare persoonlijke gezondheidsinformatie raadplegen, wijzigen of anderszins verwerken.	Beheersingsmaatregelen gericht op het borgen dat de zorginstelling een vastgesteld en geïmplementeerd beleid kent voor het verlenen van toegang tot informatie; er zijn procedures om gebruikers toegang te geven tot persoonlijke gezondheidsinformatie van patiënten die ze voor de uitvoering van hun taken nodig hebben en om onbevoegde toegang tot deze gegevens te voorkomen. Dit beleid wordt ondersteund door de inzet van technologische middelen.
3. Authenticatie	Het risico dat kwaadwillenden zich kunnen voordoen als een medewerker van de zorginstelling en daarmee onbevoegd en zonder doelbinding toegang hebben tot persoonlijke gezondheidsinformatie van patiënten.	Beheersingsmaatregelen gericht op het borgen dat authenticatie voor toegang tot persoonlijke gezondheidsinformatie van patiënten zich minimaal op het beheersingsniveau van tweefactor authenticatie (2FA) bevindt.
4. Logging	Het risico dat onbevoegde toegang tot persoonlijke gezondheidsinformatie van patiënten niet binnen redelijke termijn wordt gedetecteerd en wordt opgelost, waardoor de gevolgschade steeds groter wordt.	Beheersingsmaatregelen gericht op het borgen dat toegang die gebruikers hebben verkregen tot persoonlijke gezondheidsinformatie van patiënten is vastgelegd in logbestanden (logging). De logbestanden worden periodiek gecontroleerd op indicaties van onrechtmatige toegang of onrechtmatig gebruik van tot personen herleidbare persoonlijke gezondheidsinformatie en waar nodig wordt actie ondernomen door de verwerkingsverantwoordelijke.

Tabel 1 – aandachtsgebieden Gedragslijn inclusief inherente risico en uitwerking in de Gedragslijn

De resulteert in de volgende in NEN7510 deel 1 annex A beschreven beheersingsmaatregelen als onderdeel van de scope:

Aandachts-gebied	**Korte beschrijving van de norm (beheersings-maatregel Gedragslijn)**	**Norm (beheersingsmaatregel Gedagslijn)**
Bewustwording	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	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. Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van het beveiligingsbeleid en de -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken. Werknemers van de organisatie en, waar relevant, derde contractanten moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.
Authenticatie / Autorisatie	A.9.1.1 Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging moet worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen. Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheidsinformatiesystemen hun toegang tot persoonlijke gezondheidsinformatie beperken tot situaties: a) waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt); b) waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben; c) waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen. Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. Het beleid van de organisatie met betrekking tot toegangscontrole behoort te worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol. Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, moet professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moet de taken die worden uitgevoerd door zorgverleners en de workflow van de taak in aanmerking nemen.
Authenticatie	A.9.2.1 Registratie en afmelden van gebruikers	Een formele registratie- en afmeldingsprocedure moet worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken. 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.
Autorisatie	A.9.2.2 Gebruikers toegang verlenen	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.
Autorisatie	A.9.2.3 Beheren van speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moet worden beperkt en beheerst.
Autorisatie	A.9.2.5 Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen moeten toegangsrechten van gebruikers regelmatig beoordelen.
Autorisatie	A.9.2.6 Toegangsrechten intrekken of aanpassen	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 ze worden aangepast. 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.
Authenticatie	A.9.4.1 Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van toepassingen moet worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging. Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij tenminste twee factoren betrokken worden. De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van

		persoonlijke gezondheidsinformatie moet geïsoleerd (en gescheiden) worden van de toegang tot de informatieverwerkingsinfrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.
Authenticatie	A.9.4.3 Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer moeten interactief zijn en sterke wachtwoorden waarborgen.
Logging & Controle van Logging	A.12.4.1 Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, moeten worden gemaakt, minimaal 5 jaar worden bewaard en regelmatig worden beoordeeld.
Logging & Controle van Logging	A.12.4.2 Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden moeten worden beschermd tegen vervalsing en onbevoegde toegang. 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.

Tabel 2 – van toepassing zijnde beheersingsmaatregelen NEN7510:2017 deel 1 Annex A.

In NEN 7510:2017 deel 1 staat dat zorginstellingen de beheersingsmaatregelen selecteren op basis van de risicoanalyse en het van toepassing zijn vastleggen in de verklaring van toepasselijkheid. Voor bovenstaande beheersingsmaatregelen geldt dat deze altijd van toepassing zijn en dus in scope zijn van de assurance-opdracht. Deze beheersingsmaatregelen dienen derhalve beschouwd te worden als norm c.q. de te bereiken doelstellingen.

2.2 Scope validatie door IT-auditor in de assurance-opdracht

De scope moet in detail in het assurance-rapport worden opgenomen. Bij een assurance-opdracht moet een IT-auditor vaststellen of de scope toereikend is voor het doel van het rapport. Als dit niet het geval is, dan vermeldt de IT-auditor dit in het assurance-rapport (of brengt de IT-auditor geen rapport uit). Zie voor meer informatie richtlijn 3000 art. 24 randvoorwaarden voor de assurance-opdracht**.**

Het object van onderzoek is door de zorginstelling vastgesteld in de 0-meting en mogelijk aangescherpt in de voorbereiding van assurance-opdracht. Dit vereist dat de IT-auditor voorafgaand aan de feitelijke assurance-opdracht kennisneemt van de door zorginstelling gemaakte afwegingen ten aanzien van de scope.

Wij bevelen aan, mede gezien ook het belang van de scope voor het onderzoek en de management verantwoording, expliciet, middels een re-performance aan de hand van de in deze handreiking opgenomen beslisboom, een toetsing uit te voeren op de scope bepaling door de zorginstelling en de bevindingen van de re-performance op te nemen in het dossier behorende bij de assurance-opdracht. Voorbeelden van dossierstukken zijn de ingevulde analyse (beslisboom) en een kopie van het systeemlandschap van de zorginstelling.

Uitsluitingen (carve-out) in het assurance-rapport in verband met uitbestedingen van onderdelen die deel uitmaken van de systemen in scope is niet toegestaan zonder een toelichting op de beheersing van de uitbesteding en een vaststelling van de toereikendheid van de implementatie controls op de monitoring van de uitbesteding. Indien sprake is van (gedeeltelijke) uitbesteding van systemen die in scope zijn van de Gedragslijn, stelt de IT-auditor vast welke onderdelen zijn uitbesteed, gevolgd door het per aandachtsgebied bepalen van de impact op de aan de Gedragslijn gerelateerde beheersingsmaatregelen.

Vervolgens stelt de IT-auditor vast welke invloed de uitbesteding heeft op de beheersingsmaatregelen in relatie tot de doelstellingen van de Gedragslijn. Denk hierbij aan de toereikendheid van afspraken als vastgelegd in het contract, de SLA en de verwerkersovereenkomst, en maatregelen die zijn getroffen om de naleving hiervan vast te stellen (bijvoorbeeld incident management proces, periodieke leveranciersbeoordelingen op basis van terugkoppelingen n.a.v. de SLR-, assurance-rapporten/ ISO certificaten en de actie die op basis hiervan door de zorginstelling is genomen). Vervolgens inventariseert de IT-auditor of de beheersingsmaatregelen binnen de instelling toereikend zijn om de uitbesteding te beheersen. Ook in de situatie dat delen van de verwerking van persoonsgegevens is uitbesteed blijft de implementatie van de gedragslijn de verantwoordelijkheid van de instelling. De NVZ, als gebruiker van het assurance-rapport, wil een volledig inzicht in de implementatie van de Gedragslijn, ook in de situatie dat een deel is uitbesteed. Indien de IT-auditor constateert dat beheersingsmaatregel met betrekking tot de uitbesteding onvoldoende zijn neemt de IT-auditor dit als bevinding op in het assurance-rapport bij de

betreffende beheersingsmaatregel, en maakt de IT-auditor de afweging of dit tot een beperking van het oordeel leidt.

2.3 Uitvoering assurance-opdracht Gedragslijn toegangsbeveiliging

Voor de uitvoering van de assurance-opdracht is de Gedragslijn en het Auditkader inclusief guidance zoals opgenomen in de kolom NVZ toelichting van het Auditkader leidend. Dit is een selectie uit de NEN7510:2017 standaard annex A gericht op de aandachtsgebieden van de Gedragslijn. De in het auditkader opgenomen toetsingscriteria zijn gebaseerd op bestaande wet- en regelgeving, zoals de AVG, WGBO, KNMG en relevante NEN-standaarden.

Van de IT-auditor wordt verwacht dat hij de betrouwbaarheid in aanmerking neemt van de informatie die als assurance-informatie wordt gebruikt. De IT-auditor dient het voldoende en geschikt zijn van de afwegingen te evalueren en, indien nodig in de omstandigheden, trachten verdere assurance-informatie te verkrijgen.

De oordelen van de IT-auditor dienen in beginsel gebaseerd te zijn op de toetsingscriteria en testaanpak zoals opgenomen in de het Auditkader. De toetsingscriteria mogen evenwel niet worden beschouwd als af te vinken resultaatverplichtingen.

Indien de zorginstelling afwijkt van een toetsingscriterium neemt de IT-auditor de door de instelling uitgevoerde risicoanalyses en de geïmplementeerde alternatieve beheersingsmaatregelen in aanmerking. De IT-auditor stelt vast dat de uitgevoerde risicoanalyses toereikend is en door het management is goedgekeurd. Vervolgens stelt de IT-auditor vast of de maatregel toereikend is voor het mitigeren van het risico en stelt de IT-auditor vast dat de maatregel bestaat.

De IT-auditor is uiteindelijk zelf verantwoordelijk om vast te stellen welke testaanpak het beste past bij de onderzochte norm en de door de zorginstelling gegeven implementatie van de norm. De IT-auditor neemt hierbij de beschrijving van het risico van Tabel 1 en de beheersingsmaatregelen van Tabel 2 alsmede de toetsingscriteria en testaanpak in het Auditkader als grondslag. De testaanpak is gericht op opzet en bestaan. Dat wil zeggen interview in combinatie met observatie en inspectie zowel gericht op de control als op de betrouwbaarheid van de aangeleverde evidence.

Benadrukt wordt dat re-performance om de werking van maatregelen te toetsen geen onderdeel uitmaakt van de assurance-opdracht.

Indien op niveau van toetsingscriteria een afwijking wordt geconstateerd, dient de IT-auditor na te gaan of deze afwijking een bedreiging vormt voor het behalen van de bovenliggende (norm) beheersingsmaatregel.

Indien de professionele afweging van de IT-auditor is dat de afwijking geen bedreiging vormt voor het effectief zijn van de bovenliggende (norm) beheersingsmaatregel, stelt de IT-auditor vast dat de afwijking is vermeld in hoofdstuk 5 en heeft het geen invloed op het oordeel.

Indien de afwijking een bedreiging vormt voor het effectief zijn van de bovenliggende (norm) beheersingsmaatregel, resulteert dit in een oordeel met een beperking. De IT-auditor rapporteert in zijn oordeel de beperking met een verwijzing naar de betreffende beheersingsmaatregel. In een oordeel kunnen, afhankelijk van de uitkomst van de assurance- werkzaamheden, één of meer beperkingen worden opgenomen.

Dossiervorming en documentatie van door de IT-auditor uitgevoerde werkzaamheden dient te voldoen aan de van toepassing zijnde NOREA-richtlijnen (richtlijn documentatie 230, richtlijn 3000A) en interne kwaliteitsvereisten (kwaliteitshandboek). Het belangrijkste uitgangspunt voor het opstellen en bewaren van documentatie is dat dit zodanig plaatsvindt dat een ervaren IT-auditor die voorheen niet betrokken was bij de opdracht in staat is om inzicht te verkrijgen in de aard, de tijdsfasering en de omvang van de

werkzaamheden die zijn uitgevoerd om te voldoen aan:

- de Richtlijnen en de vereisten voortkomend uit de van toepassing zijnde wet- en regelgeving;
- de uitkomsten van de werkzaamheden en de verkregen informatie voor de onderbouwing van de uitkomst van de professionele dienst waarbij sprake is van een(eind)rapport;
- de belangrijke onderwerpen die tijdens de uitvoering van de opdracht aan het licht zijn gekomen;
- de daaruit getrokken conclusies en belangrijke vakkundige oordeelsvormingen bij het trekken van die conclusies.

Het is wenselijk hierbij aandacht te besteden aan de dossiervorming van documenten die gevoelige persoonsgegevens bevatten. De IT-auditor treft afdoende maatregelen ter waarborging van de vertrouwelijkheid van dit soort documenten door deze bijvoorbeeld geanonimiseerd op te nemen in haar dossier of te waarborgen dat deze op locatie van de zorginstelling bewaard blijven, waarbij in het IT-audit dossier de unieke identificatie en referentie van de gebruikte stukken wordt opgenomen.

Rapportage vindt plaats door middel van het model assurance-rapport behorende bij de Gedragslijn. Benadrukt wordt dat de IT-auditor zelf verantwoordelijk is om ervoor te zorgen dat het rapport voldoet aan de van toepassing zijnde NOREA-richtlijnen en het interne kwaliteitshandboek. Aan het model assurance-rapport kunnen derhalve geen rechten worden ontleend.

2.4 Oordeelsvorming

De IT-auditor heeft de opdracht gekregen om de vermelding van het management van de zorginstelling omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 te controleren en hierover assurance, met een redelijke mate van zekerheid af te geven. Het is bedoeld om de NVZ informatie te verschaffen in hoeverre de zorginstelling zorgdraagt voor de toegangsbeveiliging van digitale patiëntdossiers.

De NVZ heeft, als gebruiker van het rapport, deze keuze gemaakt enerzijds omdat zij voor het beoogd gebruik van het assurance-rapport geen detailinformatie over het onderzoeksobject nodig heeft en de instelling niet willen belasten met deze informatieverplichting. Anderzijds vindt de NVZ het belangrijk dat het management van de instelling zich bewust is van haar verantwoordelijkheid en wil dit benadrukken door de expliciete focus van de IT-auditor op de door het management afgegeven vermelding over de implementatie van de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 binnen hun instelling.

Afhankelijk van de uitkomsten van de assurance-opdracht, overweegt de IT-auditor de volgende varianten voor de oordeelsvorming.

Goedkeurend oordeel

Bij een management vermelding met of zonder gemelde tekortkomingen verstrekt de IT-auditor een goedkeurend oordeel, ook als de management vermelding afwijkingen bevat van materiaal belang, als uit de assurance-werkzaamheden met redelijke mate van zekerheid blijkt dat de management vermelding een getrouwe weergave geeft over het voldoen (opzet en bestaan) aan de Gedragslijn 1.0 voor wat betreft het onderzoeksobject. Dit conform artikel 77b van richtlijn 3000A. De IT-auditor hanteert de volgende formulering voor het oordeel in geval van goedkeuring. [Naar ons oordeel geeft de vermelding van het management van [Onderzochte Zorginstelling], in alle van materieel belang zijnde aspecten, een getrouw beeld omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 op [Onderzoeksdatum].]

De IT-auditor verwijdert vervolgens de tabel onder ‘De basis voor ons oordeel’, aangezien de management vermelding reeds een getrouw beeld geeft over het voldoen aan de Gedragslijn 1.0, inclusief de eventueel geconstateerde tekortkomingen.

Indien in de managementvermelding tekortkomingen zijn gemeld, dan wordt dit in het assurance-rapport expliciet vermeld in de volgende paragraaf:

[Benadrukking van door management geïdentificeerde afwijkingen

Wij benadrukken dat de managementvermelding naar behoren identificeert en beschrijft dat de informatie over het onderzoeksobject een afwijking [of afwijkingen] van materieel belang bevat. Dit heeft niet geleid tot een aanpassing van ons oordeel over de managementvermelding.]

Oordeel met beperkingen

Wanneer naar de professionele oordeelsvorming van de IT-auditor, de management vermelding over het onderzoeksobject geen getrouw beeld geeft over het voldoen (opzet en bestaan) aan de Gedragslijn 1.0 voor wat betreft het onderzoeksobject, doordat uit de werkzaamheden van de IT-Auditor aanvullende afwijkingen zijn gebleken van materiaal belang, die niet in de management vermelding zijn opgenomen, overlegt de IT-Auditor dit met het verantwoordelijk management van de zorginstelling. Gestreefd wordt naar een situatie waarbij de geïdentificeerde afwijking alsnog als tekortkoming in de management vermelding wordt opgenomen, zodat de IT-Auditor hierover een goedkeurend oordeel kan geven.

Indien de management vermelding geen getrouw beeld geeft over het voldoen aan de Gedragslijn 1.0 en het verantwoordelijk management van de zorginstelling is niet voornemens de vermelding te corrigeren, dient de IT-Auditor een conclusie met beperking of een afkeurende conclusie te formuleren. De IT-auditor dient een conclusie met beperking tot uitdrukking te brengen wanneer, naar de professionele oordeelsvorming van de IT-auditor, de effecten, of mogelijke effecten, van een aangelegenheid niet van dergelijk materieel belang en diepgaande invloed zijn dat er een afkeurende conclusie of een onthouding van een conclusie is vereist. De IT-Auditor hanteert de volgende tekst voor een oordeel met beperkingen.

[Naar ons oordeel uitgezonderd de aangelegenheid die staat beschreven in de paragraaf 'De basis voor ons oordeel met beperking , geeft de vermelding van het management van [Onderzochte Zorginstelling], in alle van materieel belang zijnde aspecten, een getrouw beeld omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 op [Onderzoeksdatum].]

De IT-auditor licht in de tabel onder 'De basis voor ons oordeel met beperking' toe op welke punten de management vermelding geen getrouw beeld geeft over het voldoen aan de Gedragslijn 1.0.

Afkeurend oordeel of oordeelsonthouding

De IT-auditor geeft een afkeurende conclusie of onthouding van een conclusie wanneer, naar de professionele oordeelsvorming van de IT-auditor, de management-vermelding geen getrouw beeld geeft omtrent het voldoen aan de Gedragslijninformatie en de aangelegenheid van dergelijk materieel belang en diepgaande invloed is op het voldoen aan de Gedragslijn voor wat betreft het onderzoeksobject.

Voor afkeurend oordeel hanteert de IT-auditor de volgende tekst:

[Vanwege de significantie van de afwijkingen die staan beschreven in de paragraaf 'De basis voor ons afkeurend oordeel' geeft de vermelding van het management van [Onderzochte Zorginstelling] geen getrouw beeld omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 op [Onderzoeksdatum]].

De IT-auditor licht in de tabel onder 'De basis voor ons oordeel afkeurend oordeel' toe op welke punten de management vermelding geen getrouw beeld geeft over het voldoen aan de Gedragslijn 1.0.

Voor oordeelsonthouding hanteert de IT-auditor de volgende tekst:

[Vanwege de zaken die staan beschreven in de paragraaf 'De basis voor ons oordeelsonthouding', waren wij niet in staat om voldoende en geschikte assurance-informatie te verkrijgen om een conclusie te kunnen vormen over het getrouwe beeld van de vermelding van het management van [Onderzochte Zorginstelling], omtrent het voldoen aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 op [Onderzoeksdatum]. Derhalve brengen wij hierover geen oordeel uit.]

De IT-auditor is vrij om de tabel onder 'De basis voor ons oordeelsonthouding' te verwijderen, tenzij het volgens de IT-auditor zinvol is om de beweegredenen voor haar oordeelsonthouding toe te lichten op norm niveau.

Indien de zorginstelling gebruikt maakt van een serviceorganisatie wordt de volgende paragraaf toegevoegd bij 'Aangelegenheden met betrekking tot de reikwijdte van ons onderzoek':

[Onderzochte Zorginstelling] maakt gebruik van … (naam serviceorganisatie) voor… [beschrijving geleverde diensten]. De door de [Onderzochte Zorginstelling] geïmplementeerde interne beheersingsmaatregelen met betrekking tot de uitbestede dienstverlening maken deel uit van het onderzoek.]

Indien de zorginstelling ervoor kiest om af te wijken van de toetsingscriteria, stelt de IT-Auditor vast dat dit in een risicoanalyse is uitgewerkt, door het management is vastgesteld en goedgekeurd. En vanuit de risicoanalyse alternatieve maatregelen zijn ingericht om een passend beheersingsniveau te bereiken. De IT-auditor neemt kennis van de uitgevoerde risicoanalyses en stelt vast dat deze zijn gedocumenteerd en door het management zijn goedgekeurd. Indien nodig toetst IT-auditor opzet/ bestaan van de alternatieve maatregelen (binnen de scope van de assurance-opdracht).

De IT-auditor zal eventuele tegenstrijdigheden in documentatie, interviews, waarnemingen en/of door het ontbreken van documenten in eerste instantie trachten op te lossen of tenminste te verklaren.

Bijlage 1. Model rapport implementatie Gedragslijn Toegangsbeveiliging Digitale patiëntdossiers 1.0

Deze bijlage is als separaat document verstrekt.

Bijlage 2. ‘Gedragslijn toegangsbeveiliging digitale patiëntdossiers’ versie 1.0

Deze bijlage is als separaat document verstrekt.

Bijlage 3. Auditkader ‘Gedragslijn toegangsbeveiliging digitale patiëntdossiers’ versie 1.0

Deze bijlage is als separaat document verstrekt.