Nederlandse Vereniging van Ziekenhuizen

Veel gestelde vragen 'Gedragslijn toegangsbeveiliging digitale patiëntdossiers' 1.0

Versie 1 maart 2021

Inleiding

Dit overzicht met veel gestelde vragen is onderverdeeld in de volgende thema's:
A. Algemene vragen over de NVZ Routekaart en Gedragslijn toegangsbeveiliging digitale patiëntdossiers;
B. Vragen over de 0-meting en 1-meting;
C. Inhoudelijke vragen over de Gedragslijn toegangsbeveiliging digitale patiëntdossiers;

Achter iedere vraag is tussen haakjes de publicatiedatum opgenomen en indien van toepassing de datum dat een wijziging/ aanvulling is doorgevoerd. Op deze wijze is inzichtelijk welke vragen op welk moment zijn toegevoegd of gewijzigd in dit document.

A. Algemene vragen over de routekaart
A.1. Hoe hangen de NVZ-Routekaart en de Gedragslijn toegangsbeveiliging digitale patiëntdossiers samen (20-11-2020)?
Antwoord: De Gedragslijn toegangsbeveiliging digitale patiëntdossiers is opgesteld door de NVZ en de NFU om nadere duiding te geven aan de vereisten zoals die door AVG en overige regelgeving worden gesteld aan de toegangsbeveiliging van digitale patiëntdossiers.

De NVZ Routekaart vormt het overkoepelende beleidsplan voor het implementatietraject voor de ziekenhuizen (algemeen en categoraal) om aan de informatiebeveiligingseisen ten aanzien van de toegang tot digitale patiëntdossiers te voldoen en bestaat uit twee parallelle sporen:
1. Het beleidsmatige kader gebaseerd op de door de NVZ en NFU gemaakte bestuurlijke afspraken met de Autoriteit Persoonsgegevens (AP) voor de ontwikkeling van de Gedragslijn Toegangsbeveiliging digitale patiëntendossiers (en het bijbehorende auditkader);
2. De planning van implementatie (route) van de Gedragslijn met toetsing en rapportagemomenten (0-meting/self assessment en 1-meting). De NVZ en de NFU zullen de geaggregeerde (niet tot individuele ziekenhuizen herleidbare) uitkomsten van de 1-meting delen met de AP.

A.2. Hoe kom ik aan meer (achtergrond)informatie over de het programma NVZ-routekaart en de Gedragslijn toegangsbeveiliging digitale patiëntdossiers (20-11-2020)?
Antwoord: De NVZ heeft trainingen voor de leden (interne projectleiders) aangeboden ter ondersteuning van de implementatie van de Gedragslijn en voorbereiding op de 0-meting (de self assessment). Alle documentatie is op bestuurlijk niveau gedeeld met de ziekenhuizen. De documentatie is net als deze 'Veel gestelde vragen' terug te vinden op NVZ Kennisnet via de Werkgroep Gedragslijn *Toegangsbeveiliging digitale patiëntdossiers*.

A.3. Op welke NEN 7510:2017 onderdelen is Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 van toepassing (20-11-2020)?
Antwoord: De Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 heeft alleen betrekking op de onderdelen Authenticatie, Autorisatie, Controle van logging en Bewustwording van medewerkers op het gebied van informatiebeveiliging.

De overige privacy gerelateerde elementen van *NEN 7510:2017* zullen worden uitgewerkt in versie 2.0 van de Gedragslijn. *De nader uit te werken aandachtsgebieden van NEN 7510:2017 in Gedragslijn versie 2.0 betreffen:*
- *Informatiebeveiligingsbeleid;*
- *Veilig personeel (sluiten accounts van medewerkers bij ontslag);*
- *Classificatie;*
- *Cryptografie (versleuteling);*
- *Fysieke toegangsbeveiliging;*
- *Beheer van informatiebeveiligings-incidenten.*

A.4. Stelt Gedragslijn toegangsbeveiliging digitale patiëntdossiers aanvullende eisen aan een zorginstelling ten aanzien van toegangsbeveiliging digitale patiëntdossiers (20-11-2020)?
Antwoord: Nee, het is een nadere uitwerking van de eisen ten aanzien van toegangsbeveiliging digitale patiëntdossiers. De normen zijn al bepaald in de AVG en overige regelgeving.

A.5. Wat wordt er nu verwacht van een zorginstelling ten aanzien van de Gedragslijn toegangsbeveiliging digitale patiëntdossiers (20-11-2020)?
Antwoord: Het NVZ-bestuur heeft besloten dat alle leden (algemene en categorale ziekenhuizen) in het najaar van 2020 een 0-meting (self assessment) uitvoeren, daarover een rapport opstellen en dat uiterlijk 11 januari 2021 delen met de NVZ via beveiligde e-mail aan routekaart@nvz-ziekenhuizen.nl. Voor 31 mei 2021 zal de 1-meting (assurance-opdracht) moeten worden uitgevoerd door een onafhankelijk IT Auditor (RE) en een pdf van het assurance rapport moet uiterlijk 31 mei 2021 aangeleverd zijn bij NVZ via beveiligde e-mail aan routekaart@nvz-ziekenhuizen.nl. De NVZ heeft in oktober trainingen georganiseerd en een toelichting gegeven op de NVZ Routekaart, de Gedragslijn en de 0-meting (de self assessment). De NVZ zal op basis van de uitkomsten van de 0-meting met de zorginstellingen bekijken of aanvullende ondersteuning vanuit de NVZ gewenst is.

A.6. Is de Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 een eenmalig initiatief (20-11-2020)?
Antwoord: De Gedragslijn toegangsbeveiliging digitale patiëntdossiers 1.0 is opgesteld om nadere duiding te geven aan de vereisten zoals die door AVG en overige regelgeving worden gesteld aan de toegangsbeveiliging van digitale patiëntendossiers. De verplichte audit voor de NVZ leden is eenmalig. De borging van deze informatiebeveiligingseisen wordt vormgegeven door verankering van de Gedragslijn in het information security management system (ISMS) van de instelling.

A.7. Houdt de routekaart rekening met de impact van een 2e of mogelijk 3e golf van COVID-19 op de huidige planning van de routekaart (20-11-2020)?
Antwoord: De Gedragslijn is gebaseerd op wetten en regels die al lange tijd geldig zijn en waar alle ziekenhuizen reeds aan zouden moeten voldoen. In de uitvoering van de routekaart hanteren we de planning zoals deze is vastgesteld door het NVZ-Bestuur en is gecommuniceerd naar de raden van bestuur van de ziekenhuizen. Na aanleiding van de 1e golf is de Routekaart met een half jaar uitgesteld en de NVZ houdt de ontwikkelingen nauwgezet in de gaten en zal zo nodig in overleg gaan met de AP. Zolang hierover geen alternatieve besluitvorming en communicatie plaatsvindt, wordt deze planning aangehouden (zie ook A5).

B. Vragen over de 0-meting en 1-meting

B.1. Moet een zorginstelling NEN 7510:2017 gecertificeerd zijn om aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers te kunnen voldoen (20-11-2020)?
Antwoord: Nee, de Gedragslijn toegangsbeveiliging digitale patiëntdossiers is een normenkader dat zelfstandig beoordeeld kan worden. Het normenkader is een aanvulling op NEN7510:2017.

B.2. Als een zorginstelling NEN 7510:2017 gecertificeerd is wordt dan ook automatisch aan de gedragslijn voldaan (20-11-2020)?
Antwoord: Nee, uw organisatie wordt geacht door een IT Auditor (RE) een assurance-rapportage op te laten stellen, waarmee het ziekenhuis kan aantonen aan de beschreven specifieke set van NEN7510-normen en bijbehorende toetsingscriteria van de Gedragslijn, te voldoen.

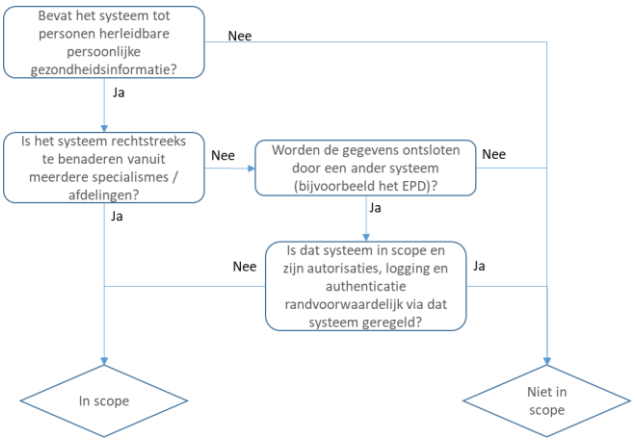
B.3. Wat valt er onder een digitaal patiëntendossier en onder een ziekenhuis breed informatiesysteem (20-11-2020, gewijzigd per 01-03-2021)?
Antwoord: Onder ziekenhuis breed informatiesysteem verstaat de Gedragslijn systemen die tot personen herleidbare persoonlijke gezondheidsinformatie bevatten, benaderbaar zijn voor meerdere specialismes en waarbij een privacy risico bestaat op ongeautoriseerde inzage buiten de behandelrelatie[1] tussen patiënt en het behandelteam.

Hieronder vallen minimaal het EPD, maar mogelijk ook 1 van onderstaande systemen:
- een EPD specifiek voor een 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)
- Medische technologie waar meerdere specialisme toegang toe hebben waaronder separate Laboratorium Informatie (Management) Systemen (LI(M)S) (zoals Labosys en Labtrain) en Radiologie Informatie / Beeldsysteem (denk aan PACS, Rogan, Carestream). Als je vanuit een EPD alleen orders kunt plaatsen van patiënten waar je een (directe) zorgrelatie hebt (labsysteem, PACS) en de uitslagen op grond van je order ontvangt in het EPD, is het labsysteem/PACS buiten scope.
- 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.

---

[1] Voor de definitie van behandelrelatie wordt verwezen naar de richtlijn van KNMG - Omgaan met medische gegevens d.d. 20-12-2019. 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. Of als toegang voor de beheersmatige afwikkeling van de behandeling noodzakelijk is.

De volgende beslisboom ondersteunt bij het bepalen of een systeem toebehoort aan het object van onderzoek.



Onder systeem verstaat de Gedragslijn een informatiesysteem waarin informatie over objecten of personen beheerd, verzameld, bewerkt, geanalyseerd, geïntegreerd en gepresenteerd kan worden. Het systeem is een geheel van front-end / applicatie, database en infrastructuur (server). De gedragslijn richt zich op toegang tot persoonlijke gezondheidsinformatie. De Gedragslijn maakt hierbij onderscheid tussen eindgebruikers en beheerders voor wat betreft autorisaties, authenticatie, logging en controle van logging.

B.4. Als een zorginstelling aan de Gedragslijn toegangsbeveiliging digitale patiëntdossiers voldoet, voldoet het dan zonder meer aan alle eisen van AP (20-11-2020)?
Antwoord: Nee, de AP hanteert alle relevante wet- en regelgeving waaronder ook de NEN 7510:2017 als kader voor haar toezicht en dat is breder dan de thema's van de Gedragslijn. Bovendien kan de AP bij een concreet toezichtonderzoek besluiten om af te wijken van de Gedragslijn. De toezichthouder zal dit wel nader moeten onderbouwen waarom wordt afgeweken van de Gedragslijn die door de ziekenhuizen zelf is opgesteld om te voldoen aan de eisen van NEN 7510:2017.

B.5. Moet de 1-meting door een gekwalificeerd IT Auditor (RE) worden uitgevoerd (20-11-2020)?
Antwoord: Zorginstelling laat een 1-meting uitvoeren door een Register EDP Auditor (RE) aan de hand van NOREA Richtlijn 3000A. De 1-meting moet voldoen aan de volgende randvoorwaarden:

- De (eindverantwoordelijk) IT Auditor moet beschikken over een RE-kwalificatie (aangesloten bij de NOREA beroepsgroep);
- De 1-meting moet volgens de Richtlijn 3000A standaard worden uitgevoerd;
- De (eindverantwoordelijk) IT Auditor moet de NVZ-training voor IT Auditors hebben gevolgd. IT-Auditors ontvangen tijdens deze training een handreiking en een templaterapport voor het uitvoeren van de 1-meting;
- Een overzicht met IT Auditors die deze training hebben gevolgd zal na afloop van de IT Audit training door NVZ worden gepubliceerd.

B.6. Moet een zorginstelling zelf afspraken maken met een auditor (20-11-2020)?
Antwoord: Ja, een zorginstelling moet zelf een afspraak maken met een IT-auditor voor het uitvoeren van de 1-meting (assurance) conform de NVZ Routekaart. Het is niet verplicht om een IT-Auditor (RE) te betrekken bij de 0-meting. De IT-Auditor (RE) kan op verzoek van het ziekenhuis worden betrokken bij de 0-meting om de norm te verduidelijken waaraan moet worden voldaan. Om haar onafhankelijkheid voor de uitvoering van de 1-meting (assessment) niet te verliezen kan de IT-Auditor die de 1-meting uitvoert, niet ondersteunen bij het ontwerpen en implementeren van maatregelen. NVZ verzorgt een training aan de auditors en beschikt over een lijst met auditors die de training hebben gevolgd.

B.7. Op welke wijze moeten ziekenhuizen onderscheid maken tussen status opzet én Bestaan, indien het onderscheid voor betreffende criterium onduidelijk is (18-12-2020)?
Antwoord: We kunnen ons voorstellen dat het niet altijd meteen eenduidig is wat het verschil tussen beide is, maar in bijna alle gevallen is dat wel te maken. Als voorbeeld het autorisatiebeleid. Opzet van het beleid is of een beleid voldoende invulling geeft aan de gestelde criteria (dit kunnen naast de Gedragslijn ook andere eisen zijn vanuit wet- en regelgeving, of wensen / eisen van stakeholders). Bestaan van het beleid betekent dat het ook eenduidig is vastgelegd, goedgekeurd en gecommuniceerd is aan de betrokkenen.
Mocht het in praktijk lastig zijn om het onderscheid tussen opzet en bestaan te maken, kies er dan voor om opzet / bestaan als geheel te toetsen (leg dan in kolom opzet en bestaan hetzelfde resultaat vast).

B.8. Hoe geven we de status nuancering per scope onderdeel aan: van sommige toetsingscriteria is de status van EPD “voldoet”, maar zijn er deelsystemen die een lagere status hebben *(18-12-2020)*?
Antwoord: Het totaaloordeel is het laagste oordeel van de individuele systemen in scope. Dus geen oordeel per systeem als de scope uit meerdere systemen bestaat.

Zorginstelling is hierbij vrij om in de beschrijving van de actie in het self assessment rapport of in de beschrijving van de bevinding in het onderliggende auditkader aan te geven dat het specifiek betrekking heeft op 1 systeem en niet alle systemen in scope. Bij 1-meting zal ook de auditor gevraagd worden om ‘voldoet niet’ bevinding (afwijking) zonodig nader te specificeren.

B.9. Wat verstaat de Gedragslijn onder de term 'voor meerdere specialisme toegankelijk' (18-12-2020, gewijzigd per 01-03-2021)?
Antwoord: Dat zijn systemen waar meerdere specialismen in samen (kunnen) werken en waarbij een verhoogd privacy risico bestaat op ongeautoriseerde raadplegingen (buiten de definitie van directe behandelrelatie) van tot personen herleidbare persoonlijke gezondheidsinformatie. Dit risico neemt toe naar mate meerdere specialismes/ afdelingen toegang hebben, zonder te beschikken over een directe behandelrelatie met de patiënt of betrokken te zijn bij de administratieve afhandeling van de behandeling.

B.10 Klopt het dat een auditor niet de 0-meting kan verzorgen (18-12-2020)?
Antwoord: In de standaardrapportage die beschikbaar is gesteld voor het uitvoeren van de 0-meting wordt ervan uitgegaan dat het verantwoordelijk management/ Raad van Bestuurslid verantwoordelijkheid neemt voor de rapportage en deze ondertekent. Het is zeker wel mogelijk om delen van de werkzaamheden te laten uitvoeren door een externe partij, ook de beoogde RE voor de 1-meting. Deze RE moet dan uiteraard wel, om zijn onafhankelijkheid te

behouden, niet betrokken zijn bij het oplossen van de eventueel geconstateerde tekortkomingen. De beoogde RE voor de 1-meting mag voor de 0-meting ook om uitleg bij de normen worden gevraagd.

B.11 Klopt het dat de auditor tijdens de 1-meting de vermelding van het management dient te beoordelen, in plaats van het beoordelen per norm of we aan de Gedragslijn voldoen (18-12-2020, gewijzigd per 01-03-2021)?
Antwoord: De NVZ heeft aangegeven dat de 1-meting die door de IT Auditor een zogenaamde 3000 Attest onderzoek is, de IT Auditor onderzoekt of het onderzoeksobject voldoet aan de criteria (de Gedragslijn Toegangsbeveiliging Digitale Patiëntdossiers) door de vermelding van het management van de instelling over de implementatie van de Gedragslijn Toegangsbeveiliging Digitale Patiëntdossiers te onderzoeken. Dit is een onderzoeksaanpak die in toenemende mate wordt toegepast, ook de VIPP5 regeling zal getoetst worden volgens een 3000A aanpak.

Het verantwoordelijk management van de instelling moet dus inderdaad zelf vaststellen dat ze voldoen aan de criteria, anders is zij niet in staat een management vermelding van of namens het eindverantwoordelijk management af te geven. De IT Auditor moet vaststellen dat het management (RvB) terecht concludeert dat aan de gedragslijn wordt voldaan. De IT-auditor moet voldoende betrouwbaar bewijs verzamelen om zelfstandig een oordeel te vormen over de implementatie van de Gedragslijn Toegangsbeveiliging Digitale Patiëntdossiers op basis van de in het auditkader gegeven criteria, hierbij kan de IT-auditor gebruik maken van het bewijs dat voortkomt uit door het management van de instelling (of een derde) uitgevoerde controles op de implementatie van de gedragslijn.
Als de IT Auditor zo veel mogelijk gebruik wil maken van de informatie uit de door of namens het management uitgevoerd controls dan kan deze:

- Vaststellen hoe het eindverantwoordelijk management tot zijn conclusie komt
- De conclusie en de onderbouwing (dossier) daarvan reviewen
- Afhankelijk van de risicoschatting van de IT Auditor meer of minder re-performance doen (zelf nogmaals vaststellen of aan bepaalde elementen van de gedragslijn inderdaad wordt voldaan)

De noodzakelijke inspanning van de IT Auditor zal sterk afhangen van de kwaliteit van het ingevulde auditkader van de zorginstelling en de onderbouwing en de dossiervorming van hoe het management tot zijn conclusie komt. Dat zal trouwens ook invloed hebben op de risico inschatting van de IT Auditor. Keuze voor de onderzoeksaanpak zal gemaakt worden op basis van wat voor de IT Auditor haalbaar en de meest efficiënte werkwijze is.

B.12 Toetst de IT-auditor in de 1-meting de Gedragslijn of het interne beleid (01-03-2021)?
Antwoord: Beiden. De IT-auditor toetst het beleid om vast te stellen dat het beleid in opzet voldoet aan de Gedragslijn. Vervolgens toetst de IT-Auditor het bestaan van het beleid.

De zorginstelling dient ten alle tijden te waarborgen dat het, naast relevante wet- en regelgeving, voldoet aan haar eigen intern vastgestelde beleid (“practice what you preach”). Indien de instelling niet conform haar eigen beleid handelt, bestaat het risico dat dit door een onafhankelijke beoordeling van een auditor of toezichthouder als een afwijking wordt beschouwd, ook als dit niet direct in strijd is met geldende wet- en regelgeving. De zorginstelling doet er daarom verstandig aan haar intern beleid (opzet) niet mooier voor te

spiegelen dan de werkelijkheid is. Het beleid dient wel minimaal aan geldende wet- en regelgeving te voldoen (zie ook OLVG boetebesluit).

C. Inhoudelijke vragen over de Gedragslijn

Algemeen

C.1. Welke richtlijnen zijn er voor het uitvoeren van een risicoanalyse (20-11-2020)?
Antwoord: in de toelichting op de Gedragslijn (trainingsslides NVZ Routekaart – implementatie gedragslijn training ziekenhuis) wordt een nadere toelichting gegeven op het uitvoeren van een risicoanalyse inclusief een voorbeeld.

C.2. Kan de NVZ good practices delen voor het verder invullen van de Gedragslijn, bijvoorbeeld voor de inrichting van autorisaties i.r.t. de definitie van de behandelrelatie (20-11-2020)?
Antwoord: De NVZ heeft op NVZ Kennisnet de Werkgroep *Gedragslijn toegangsbeveiliging digitale patiëntdossiers* ingericht, waarop ziekenhuizen onderling kennis en good practices kunnen uitwisselen. Hier kunnen alle deelnemers van de trainingen, projectleiders en andere belangstellenden samenwerken en kennis / ervaringen uitwisselen. Daarnaast zal NVZ dit document met veel gestelde vragen periodiek bijwerken en publiceren op het Kennisnet en actuele informatie delen met de leden.

C.I. Bewustwording

Geen vragen tot nu toe.

C.II. Autorisaties en Authenticatie

C.II.1. In de Gedragslijn staat: "De organisatie hanteert voor interne toegang tot persoonlijke gezondheidsinformatie MFA, tenzij het verantwoordelijk management afwijkend beleid voor toegang tot persoonlijke gezondheidsinformatie heeft vastgesteld." Mag het management in haar beleid 1-factor authenticatie voorschrijven (20-11-2020)?
Antwoord: Nee, dat is niet toegestaan. Dit punt moet in samenhang worden gelezen met de onderliggende bullits in de Gedragslijn. Daarin staat vermeld bij bullit 1: "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)."

En bij bullit 2: "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."

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 management *vastgesteld* en *goedgekeurd*. Vanuit de risicoanalyse zijn *alternatieve maatregelen* beschreven en ingericht om *een passend beheersingsniveau* te bereiken.

C.II.2. *Is Gracing (het meenemen van een sessie gedurende een bepaalde periode met 1-factor) zonder meer toegestaan (20-11-2020)?*
Antwoord: Nee, dit is een afwijking op het MFA-beleid. Hiervoor geldt hetzelfde als bij de vorige vraag. Er moet een *gegronde reden* (stand der techniek, patiëntveiligheid, infectiepreventie, etc.) 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.

C.II.3. Is het gebruik van een noodprocedure (Breaking the Glass) verplicht (20-11-2020, gewijzigd per 01-03-2021)?
Antwoord: nee, dit is niet verplicht. Kern van de Gedragslijn is het inregelen van een goede balans tussen de preventieve inrichting van een adequaat autorisatiebeleid in de systemen (zijn de autorisaties op inzage van tot personen herleidbare persoonlijke gezondheidsinformatie rechtmatig) en de detectieve uitvoering van controles op de logging (hebben medewerkers hun autorisaties in de systemen rechtmatig toegepast). De noodprocedure functionaliteit is een maatregel, waarmee hier invulling aan kan worden gegeven. Maar alternatieve invulling is ook denkbeeldig.

C.II.4. Wat verstaat de Gedragslijn onder speciale bevoegdheden (20-11-2020, gewijzigd per 01-03-2021)?
Antwoord: Vervallen. Zie C.II.7

C.II.5 *Wordt het gebruik van netwerkzonering (locatie) gezien als geldige 1e of 2e factor (20-11-2020)?*
Antwoord: Nee, in de gedragslijn definiëren we MFA als volgt: MFA (Multi Factor Authenticatie), authenticatie methode 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. Het netwerk (zonering) wordt niet als authenticatie factor gezien.

Wel kan zonering als een van de alternatieve maatregelen worden ingezet bij het uitvoeren van risicoanalyses, bijvoorbeeld bij het gebruik van 'gracing' op bepaalde afdelingen. Hier moet ten eerste sprake zijn van een gegronde reden om af te wijken. Vervolgens dient door middel van risicoanalyse alternatieve maatregelen worden ingericht om tot eenzelfde of passend beheersingsniveau te komen.

C.II.6 *Bij Norm 9.1.1 punt c: "Gebruikers en dienstverleners behoren een duidelijke instructie te ontvangen waarin is vastgelegd aan welke bedrijfseisen de toegangsbeveiligings-maatregelen moeten voldoen." Wie wordt in deze context bedoeld met 'dienstverleners'? Worden hier inhuurkrachten bedoeld die gebruik maken van het systeem en/of wordt hier ook de leverancier van het systeem bedoeld. Is dat laatste niet het geval, wordt toegang door de leverancier dan überhaupt gedekt door het normenkader (01-03-2021)?*

Antwoord: De Gedragslijn richt zich op toegang tot persoonlijke gezondheidsinformatie. Onder gebruikers en dienstverleners worden dus ook inhuurkrachten, PNIL (bijvoorbeeld vrijwilligers) en leveranciers bedoeld, voor zover zij logische en rechtmatige toegang hebben tot de persoonlijke gezondheidsinformatie van patiënten in het ziekenhuisbrede informatiesysteem. Leveranciers die geen toegang hebben tot systemen die tot personen

herleidbare persoonlijke gezondheidsinformatie bevatten, zijn voor de Gedragslijn niet in scope.

C.II.7 Bij Norm 9.2.3 BEHEREN VAN SPECIALE TOEGANGSRECHTEN: Wij veronderstellen dat hier OOK database beheerrechten worden verstaan? Of enkel de speciale toegangsrechten BINNEN de applicatie (01-03-2021)?

Antwoord: onder speciale beheerrechten worden zowel de speciale rechten binnen de applicatie bedoeld (denk aan functioneel beheerders, key users of medewerkers met meer rechten dan noodzakelijk in het kader van de behandelrelatie of administratieve afhandeling) als de rechten op database / OS-niveau voor zover hiermee toegang kan worden gekregen tot persoonlijke gezondheidsinformatie van patiënten. De organisatie voert periodiek aanvullende controles uit, geautomatiseerd en/of gerichte deelwaarneming, bovenop de steekproef van 60 om te borgen dat er een systematiek is geïmplementeerd, waarmee het risico op onrechtmatig gebruik van autorisaties om tot personen herleidbare persoonlijke gezondheidsinformatie in te zien tijdig kan worden gedetecteerd en gecorrigeerd[2]. (zie ook vraag C.III.3)

C.III. Logging

C.III.1. Waarom is er verschil in/keuze gemaakt voor procesgerichte en een gegevensgerichte controle en een verschil in/keuze gemaakt voor deelwaarneming en steekproef in geval van logging controle op de noodprocedure (breaking the glass) respectievelijk toegang tot patiëntendossiers (20-11-2020)?
Antwoord: De noodprocedure is een gedefinieerd proces. Voor het toetsen van een proces is een procesgerichte controle d.m.v. deelwaarneming de vaktechnische norm. 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.

C.III.2. Bij de controle van de logresultaten van de noodprocedure staat 60 gebeurtenissen of 60 deelwaarnemingen beschreven. Bij de logging van de toegang tot patiëntdossiers staat een steekproef van 60 patiëntendossiers beschreven. Wat wordt verstaan onder het aantal van 60 patiëntendossiers. Zijn dat echt inhoudelijk 60 patiëntdossiers of 60 logregels (20-11-2020)?
Antwoord: Voor noodprocedure betreft het een selectie van zestig (60) gebeurtenissen (risicogericht, zie antwoord *C.III.1.*).

Voor andere toegang tot patiëntdossiers dienen zestig (60) dossiers d.m.v. een aselecte steekproef te worden gecontroleerd, waarbij alle gebeurtenissen van het afgelopen jaar worden onderzocht. De aselecte steekproef kan worden uitgevoerd d.m.v. een random functie of steekproefsoftware. Let op, via het Internet zijn steekproefprogramma's beschikbaar. Deze kunnen gebruikt worden, mits hierin alleen regelnummers en niet tot personen herleidbare gegevens worden meegegeven i.v.m. de privacywetgeving.

---

[2] Zie OLVG boetebesluit met als uitgangspunt van de AP dat de controle van de logging systematisch en consequent moet plaatsvinden, waarbij een steekproefsgewijze controle en/of controle op basis van klachten niet voldoende is (https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_olvg.pdf)

C.III.3. Bij de controle van de toegang op patiëntdossiers wordt gesproken over een homogene massa. De vraag is of er sprake kan zijn van een homogene massa. Er is grote diversiteit binnen een groep patiënten (denk aan VIP's, collega medewerkers die patiënt zijn, inactieve en actieve patiënten (wel/niet actueel in behandeling), overleden/niet-overleden patiënten, et cetera) (20-11-2020, gewijzigd per 01-03-2021).
Antwoord: 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. Voor noodprocedure betreft het een selectie van zestig (60) gebeurtenissen (risicogericht, zie antwoord *C.III.1.*). Omdat in de controle van de noodprocedure risicogericht selectie plaatsvindt, volstaat het om de andere toegang tot patiëntdossiers te beschouwen als een homogene massa en hierop een aselecte steekproef uit te voeren van minimaal zestig (60) patiëntdossiers. Uitgangspunt hierbij 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 minimum aantal 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 beheersingsmaatregelen. Passende beheersingsmaatregelen zijn bijvoorbeeld het periodiek uitvoeren van aanvullende controles (geautomatiseerd en/of gerichte deelwaarneming) bovenop de steekproef van 60 om te borgen dat er een systematiek is geïmplementeerd waarmee het risico op onrechtmatig gebruik van autorisaties om tot personen herleidbare persoonlijke gezondheidsinformatie in te zien tijdig kan worden gedetecteerd en gecorrigeerd (zie ook OLVG boetebesluit).

C.III.4. Moet in de gedragslijn ook nog melding worden gemaakt van gerichte controles op verzoek van bijvoorbeeld een patiënt (20-11-2020)?
Antwoord: In het kader van de AVG-wetgeving heeft iedere patiënt het recht om een informatieverzoek in te dienen. Dit is een separaat proces dat losstaat van de interne controle op logging.

C.III.5. In het auditkader staat "Stel voor één testpatiënt in de logging vast dat de gebeurtenis wordt gelogd als de noodprocedure voor deze patiënt wordt geactiveerd." Is het zich toegang verschaffen tot een patiëntdossier t.b.v. deze audit rechtmatig (20-11-2020)?
Antwoord: Gesproken wordt hier over een *testpatiënt* en geen echte patiënt. Het zich toegang verschaffen tot een patiëntdossier t.b.v. deze audit is niet de bedoeling. Deze test dient derhalve op een niet naar een natuurlijk persoon herleidbare *testpatiënt* te worden uitgevoerd.

C.III.6. Hoe controleer je de logging indien het autorisatiemodel en de noodprocedure (breaking the glass) niet 100% sluitend is ingericht (20-11-2020, gewijzigd per 01-03-2021)?
Antwoord: Hiervoor is de algemene 'Controle van de logging van toegang tot patiëntdossier', zoals beschrijven in bijlage 3 van de Gedragslijn bedoeld en C.III.3.

C.III.7 Voor Logging en controle van de logging, ligt dan de scope, voor wat betreft de Gedragslijn, alleen bij het EPD (18-12-2020)?
Antwoord: Ook de criteria voor wat betreft logging betreffen alle systemen die in het object van onderzoek vallen, dus dat kan breder zijn dan het EPD.

Voorbeeld van systeem naast het EPD scenario 1: Betreffende ziekenhuisbrede informatiesystemen worden via het EPD ontsloten en raadplegingen worden via de logging functionaliteit van het EPD gelogd. De systemen zijn niet door meerdere specialismes direct te benaderen. Dan is de scope van de Gedragslijn voor logging (en ook autorisaties/authenticatie) het EPD.

Voorbeeld van systeem naast het EPD scenario 2: Betreffende ziekenhuisbrede informatiesystemen zijn door meerdere specialismes direct te benaderen (buiten het EPD). Dan moeten autorisaties, authenticatie en logging in het systeem geborgd zijn. Indien dit bijvoorbeeld door stand der techniek niet mogelijk is (denk aan legacy systemen) voert de instelling een risicoanalyse uit en treft passende alternatieve beheersingsmaatregelen.

C.III.8 Wat is de impact van geconstateerde afwijkingen op de steekproefomvang en welke vervolgwerkzaamheden voert de zorginstelling uit bij geconstateerde afwijkingen (18-12-2020)?
Antwoord: De doelstelling van het gebruik van steekproeven is om enerzijds een onderbouwing te geven van het aantal te controleren steekproeven en anderzijds een gedegen grondslag te leggen voor conclusies over de gehele populatie waaruit de steekproef is getrokken. De tabel in bijlage 3 van de Gedragslijn biedt een hulpmiddel om voor verschillende betrouwbaarheidsvereisten en verschillende foutverwachtingen de omvang van de steekproef te bepalen. Als voorbeeld is in de Gedragslijn een omvang van 60 gegeven, uitgaande van 95% betrouwbaarheid, 5% nauwkeurigheid en 0 verwachte fouten. De 0 verwachte fouten hypothese hanteer je als je 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)

Het uiteindelijke doel van de controle van logging is om als organisatie te leren van geconstateerde afwijkingen en verbeteringen door te voeren om in de toekomst dergelijke afwijkingen te voorkomen.