Factsheet 2

IV Wvggz

1. Inleiding en doel factsheet

De Wet verplichte geestelijke gezondheidszorg (Wvggz) treedt in werking op 1 januari 2020. Gemeenten bereiden zich voor op deze nieuwe wet. Ook in ketenverband wordt hard gewerkt om de wet vanaf de startdatum goed uit te kunnen voeren. De VNG maakt periodiek een factsheet over de informatievoorziening die nodig is om de uitvoering van de Wvggz te ondersteunen. De doelgroep van deze factsheet zijn degenen die vanuit gemeenten bezig zijn met de informatievoorziening (IV) van de Wvggz. Dit is de tweede factsheet over de IV van de Wvggz. De eerste factsheet is – samen met veel andere informatie over de wet – te vinden op vng.nl onder Wvggz.

Deze factsheet kent de volgende opbouw:

- Veilige mail: keuze voor een voorziening
- Harmonisatie beveiligingsmaatregelen
- Veelgestelde vragen / FAQ
- Bijlage: Organisatorische eisen vanuit NTA

Daarnaast vormen de volgende twee documenten als apart bestand ook een bijlage bij deze factsheet:

1. Document van de firma Khonraad over het voldoen aan het 'Harmonisatiedocument Informatiebeveiliging'
2. Eerste versie FAQ gemaakt door de firma Khonraad

De inhoud van deze factsheet is afgestemd met de gemeentelijke werkgroep IV-Wvggz, waarin momenteel deelgenomen wordt door de gemeenten Utrecht, Den Bosch, Ede, Arnhem, Den Haag en BAR. Ook is afgestemd met de firma Khonraad en het ketenprogramma Wvggz.

Voor meer informatie over de Wvggz kunt u ook gebruik maken van de handreikingen voor de crisismaatregel, het verkennend onderzoek en de implementatie van de Wvggz. Meer informatie hierover vindt u op de website van de VNG. Daarnaast is er informatie beschikbaar op de website www.dwangindezorg.nl.

2. Veilige mail: keuze voor een voorziening

Waar heeft een gemeente veilige mail voor nodig in de Wvggz?

Veilige mail wordt gebruikt in de informatie-uitwisseling met ketenpartners ten behoeve van de Wvggz, deels vanuit het reguliere scenario (i.e. als alles werkt zoals het moet) en deels vanuit 'plan B' (i.e. als een deel van de IV uitvalt of niet beschikbaar is).

In deze factsheet geven we aan hoe gemeenten een keuze kunnen maken voor een voorziening voor veilige mail. Dit doen we vanuit het reguliere scenario. Zodra de werkwijze voor Plan B in ketenperspectief duidelijk is, kan ook voor Plan B beoordeeld worden welke rol veilige mail daarin speelt. We verwachten dat veilige mail (ook) in plan B een belangrijke rol zal spelen. Daarop komen we in een volgende factsheet terug. We komen later ook terug op de vraag hoe een gemeente de te gebruiken voorziening voor veilige mail kan inrichten voor gebruik binnen de Wvggz. Over dit onderwerp, i.e. het operationaliseren van veilige mail voor de Wvggz, verschijnt in september een werkdocument met praktische informatie, dat in ketenverband is opgesteld.

Eerst geven we aan waar veilige mail binnen de Wvggz precies voor nodig is en welke keuzes gemeenten daarin kunnen maken. Dit doen we door kort de verschillende informatiestromen te verkennen. In het reguliere scenario zullen, voor zover we nu kunnen inschatten en wetende dat er nog verschillende overleggen lopen over de gewenste IV, de informatiestromen als volgt lopen:

- In de samenwerking rondom de **crisismaatregel** wordt met ketenpartners gecommuniceerd via systeemkoppelingen en met de Berichtenbox van het Khonraad systeem. Het is dus de firma Khonraad die deze informatiestromen inricht. Dit geldt voor communicatie met de GGZ, het OM, de IGJ, de Raad voor Rechtsbijstand en zorgverleners / zorgaanbieders. Ook het versturen van de **aanvraag voor het voorbereiden van een zorgmachtiging** aan het OM wordt door firma Khonraad ingericht. Daarnaast zal communicatie vanuit de Rechtbank naar gemeenten in eerste aanleg per post worden verzorgd. Voor communicatie met al deze ketenpartners hebben gemeenten dus geen aparte veilige mailvoorziening nodig.
- De enige uitzondering hierop lijkt mogelijk de communicatie met de gezinsvoogdijmedewerker. Indien de organisatie waar de gezinsvoogdijmedewerker werkt aangesloten is of wil worden op de Berichtenbox, dan kan deze voorziening gebruikt worden en is geen aparte veilige mail voorziening nodig. Als de organisatie van de gezinsvoogdijmedewerker dat niet wil, zal een ander communicatiekanaal gekozen moeten worden. Dat kan veilige mail zijn, maar ook per post is dan een optie.
- Naast de hierboven benoemde en in de wet beschreven partners waarmee informatie uitgewisseld wordt in het kader van de Wvggz, kan er – met name voor het uitvoeren van het **verkennend onderzoek** – ook informatie uitgewisseld worden met partijen die niet expliciet in de wet benoemd zijn. Dit kan bijvoorbeeld afdelingen van de gemeente betreffen, alsook de wijkagent (politie), het wijkteam, het veiligheidshuis, etc. Ook voor deze communicatie is veilige mail een werkbare optie.
- Gemeenten kunnen er daarnaast voor kiezen om via veilige mail met **burgers** te communiceren. Burgers kunnen daarbij verschillende rollen hebben, waaronder melder, betrokkene of vertegenwoordiger. De wet laat communicatie met burgers vormvrij, behoudens de verplichting om een aantal informatieproducten schriftelijk kenbaar te maken. Gemeenten kunnen dus kiezen of ze veilige mail inzetten voor communicatie met burgers; dat hoeft niet.

Conclusie over de noodzaak voor het gebruik van veilige mail:

- Gemeenten hebben voor de uitvoering van de Wvggz een veilige mail voorziening nodig, naast het gebruik van het systeem van de firma Khonraad en de Berichtenbox die daarbij hoort.
- Voor gemeenten is in het reguliere scenario een externe voorziening voor veilige mail nodig voor communicatie met 'andere partijen' in het verkennend onderzoek.
- Gemeenten die dat willen (dit betreft een keuze binnen beleidsvrijheid) kunnen via mail met burgers communiceren.
- Communicatie met de gezinsvoogdijmedewerker kan indien gewenst per veilige mail gebeuren; ook dit is een keuze voor de gemeente.

Aansluiten externe voorziening op de Berichtenbox van Khonraad

Veelal zal de gemeente voor de Wvggz werken vanuit het systeem van Khonraad, zowel voor de crisismaatregel als voor het verkennend onderzoek in het traject van zorgmachtigingen. Het is daarom een relevante vraag hoe veilig mailen straks werkt in samenhang met het Khonraad-systeem. Een belangrijke schakel hierin is de Berichtenbox van Khonraad.

De Berichtenbox van Khonraad is een functionaliteit voor het versturen en ontvangen van veilige mailberichten in een besloten groep (van alléén bekende personen). Met de Berichtenbox kan zowel ongestructureerde als gestructureerde informatie gedeeld worden. Als je een account voor het Khonraad systeem hebt, dan krijg je automatisch ook de mogelijkheid om de Berichtenbox van Khonraad te gebruiken.

Via de Berichtenbox kun je dus veilig berichten uitwisselen (lees: mailen) met personen en instanties die ook toegang hebben tot de Berichtenbox. Het gaat daarbij zowel om het verzenden als om het ontvangen van berichten.

Soms is het uiteraard ook nodig of wenselijk om een bericht te sturen aan iemand die zelf geen Berichtenbox heeft, bijvoorbeeld een burger. Mails aan personen die geen Berichtenbox account hebben, kunnen vanuit Khonraad verzonden worden en worden afgeleverd aan de burger via een externe / commerciële veilige mail-voorziening die daaraan gekoppeld wordt. Daar heb je als gemeente dus een aparte voorziening voor veilige mail voor nodig.

Hierbij dient nog opgemerkt te worden dat hier alleen het verzenden van berichten wordt gefaciliteerd, niet het ontvangen. Dit wordt ook toegelicht in de FAQ van de firma Khonraad die als bijlage bij deze factsheet is bijgevoegd. Als de geadresseerde een retourbericht wil sturen aan de verzender (vanuit een gemeente), dan zal daarvoor een ander kanaal gebruikt moeten worden, bijvoorbeeld veilige mail. Het is dan aan de medewerker van de gemeente om de op die manier ontvangen informatie waar nodig in het Khonraad systeem te zetten met 'drag en drop'.

Ketenafspraken over veilige mail

Iedere gemeente kan kiezen welke externe voorziening voor veilige mail gebruikt zal worden. Wel is hierover in ketenverband afgesproken dat we alleen voorzieningen gebruiken die (gaan) voldoen aan de juiste norm. Dit wordt toegelicht in deze sectie.

Onder initiatief van het Informatieberaad Zorg is door de NEN een norm gepubliceerd voor het e-mailen van persoonlijke gezondheidsinformatie in de zorg: de NTA 7516.

https://www.informatieberaadzorg.nl/actueel/nieuws/2019/05/15/norm-voor-e-mailen-in-de-zorg-gepubliceerd

Als organisaties en het product dat zij gebruiken voor e-mailen voldoen aan de norm, dan voldoen zij aan de veiligheidseisen die zijn gesteld aan het mailen van persoonlijke gezondheidsinformatie.

Producten die voldoen aan de norm zullen ook interoperabel zijn. Dat wil zeggen dat mails tussen producten van leveranciers onderling worden doorgegeven zodat ze op het product dat de ontvanger gebruikt binnenkomen. Daarmee vervalt de administratieve overlast die nu bestaat als de ontvanger niet hetzelfde mailproduct gebruikt als de verzender.

De samenwerkende organisaties in het programma Wvggz hebben (in de bestuurlijke ketenraad BKR) de norm omarmd en afgesproken dat organisaties die een rol hebben in de uitvoering van de Wvggz streven naar het zo spoedig mogelijk zelf aan de norm voldoen én een NTA gecertificeerd veilige mail product zullen gebruiken bij de uitvoering van deze wet. Bij voorkeur al vanaf het moment dat de wet in werking treedt (1 januari 2020), maar anders zo spoedig mogelijk daarna.

In december 2018 heeft een aantal productleveranciers en aanbieders van veilige mail diensten een intentieverklaring getekend. Zie bovenstaande link voor de namen van deze organisaties. In de intentieverklaring spreken zij uit binnen één jaar na publicatie te voldoen aan de norm. De norm is op 16 mei 2019 gepubliceerd door de NEN.

Er is op dit moment nog geen enkele leverancier die aan de NTA 7516 voldoet. Eén van de belangrijkste eisen die gesteld wordt is namelijk dat de verschillende oplossingen interoperabel zijn. Dat is functioneel in de NTA wel vastgesteld, maar er is nog geen overeenstemming over hoe dat technisch opgelost wordt. Pas als die overeenstemming er is, kunnen leveranciers die afgesproken oplossing implementeren.

In de NTA is afgesproken dat leveranciers pas publiekelijk mogen aangeven dat ze aan NTA 7516 voldoen als ze daarvoor een certificaat hebben gehaald. Op dit moment wordt er nog gewerkt aan de manier waarop dat certificeringstraject eruit moet zien. Onder toezicht van het Informatieberaad Zorg zullen producten van leveranciers worden gecertificeerd. De datum waarop producten gecertificeerd zullen zijn is nog niet bekend, maar de verwachting is dat begin 2020 de eerste producten zijn gecertificeerd.

Omdat deze datum na de datum van inwerkingtreding van de Wvggz ligt hebben we te maken met een overgangsperiode. Daarom probeert het ketenprogramma Wvggz vooruitlopend op de certificering inzicht te krijgen in welke productleveranciers wellicht al voor 1 jan 2020 aan de elementen uit de norm kunnen voldoen, zonder de certificering maar wel met de interoperabiliteit. Op het moment van schrijven is van een viertal productleveranciers bekend dat zij samenwerken om dit voor elkaar te krijgen. Dat zijn ZorgMail, Zivver, Cryptshare en Khonraad; ook KPN heeft zich gemeld bij het ketenprogramma.

Organisaties (en dus ook gemeenten) moeten zelf bepalen hoe en wanneer zij de beschikking hebben over een product voor veilig mailen dat (op korte termijn) voldoet aan de norm. In de BKR is afgesproken dat organisaties proberen al op 1 oktober 2019 de beschikking te hebben over een veilige en interoperabele mail oplossing. Vaak hebben organisaties al één of meer producten in huis. Het is dan zaak om contact op te nemen met de leverancier om te bespreken of en wanneer hij zijn product zal laten voldoen aan de NTA 7516, of deze al eerder aan de vereiste van interoperabiliteit kan voldoen en wat er nog nodig is om die versie van het product te implementeren (technisch en organisatorisch).

Vanuit het project Veilige Mail van het Informatieberaad Zorg komt deze zomer een implementatiehandboek en zij hebben de intentie om de planning inzichtelijk te maken van productleveranciers om te gaan voldoen aan de norm.

Mocht het nodig zijn om een product te verwerven / kopen, dan is het raadzaam om het (gaan) voldoen aan de NTA 7516 (gecertificeerd zijn) als harde eis te hanteren bij de selectieafweging.

Het selecteren van een voorziening voor veilige mail

Naast de hierboven beschreven eis dat de te gebruiken veilige mail voorziening voldoet aan de NTA 7516, is het voor gemeenten ook van belang dat de gekozen voorziening tijdig aan het Khonraad systeem gekoppeld kan worden, om per 1-1-2020 operationeel te zijn. Khonraad werkt nu aan aansluiting met Zivver en ZorgMail en er loopt een proof of concept met Cryptshare. Welke andere leveranciers ook tijdig op Khonraad aangesloten (kunnen) gaan worden is nu nog niet duidelijk, en hangt ook af van de wensen die gemeenten daarover aan Khonraad kenbaar gaan maken.

Voor het kunnen gebruiken van veilige mail voor de Wvggz, zijn voor gemeenten dus twee aspecten van belang:

1. Voldoet de voorziening aan de NTA?
2. Kan de voorziening tijdig gekoppeld worden aan het Khonraad systeem?

Vanuit deze 2 aspecten kunnen gemeenten de volgende keuzes maken:

- Als je al een leverancier gecontracteerd hebt die heeft aangegeven te zullen voldoen aan de NTA, dan kan je via die leverancier ook de Wvggz-communicatie doen.
  - Ga in dat geval na of het contract met de leverancier dekkend is voor het beoogde gebruik in het kader van de Wvggz. Dit betreft bijvoorbeeld de vraag of de juiste personen de beschikking krijgen over de voorziening.
  - En ga bij Khonraad na of de voorziening tijdig op het systeem van Khonraad aangesloten kan worden.
  - Mocht je als gemeente een andere leverancier willen gebruiken, stem dan tijdig af met Khonraad. De wens van firma Khonraad is om dit voor 15 oktober 2019 te doen.
- Als je nog geen leverancier gecontracteerd hebt die per 1-1-2020 zal voldoen aan de NTA, dan heb je als gemeente een keuze:
  - Ga in overleg met je huidige en/of voorkeursleverancier alsook met Khonraad om te bezien of deze leverancier per 1-1-2020 kan voldoen aan de NTA en tijdig op het CM-systeem aangesloten kan worden.
  - Of, selecteer en contracteer een leverancier waarvan al bekend is dat ze tijdig aan de norm zal voldoen en aangesloten zal zijn op Khonraad. Hierbij kan het een optie zijn om een tijdelijk abonnement of een abonnement voor een beperkt aantal gebruikers te vragen, alleen voor de Wvggz.

3. Khonraad voldoet aan Harmonisatiedocument Informatiebeveiliging

Het verlenen van verplichte zorg is voor betrokkenen een ingrijpende gebeurtenis. En in de werkprocessen rondom die verplichte zorg worden gevoelige persoonsgegevens verwerkt. Het is daarom van groot belang dat de informatiebeveiliging op orde is. Daarom is er vanuit het ketenprogramma een 'Harmonisatiedocument informatiebeveiliging' opgesteld waarin beschreven is aan welke eisen de werkwijzen en informatievoorziening moeten voldoen.

Gemeenten moeten geregeld rapporteren over de informatievoorziening die zij gebruiken, en specifiek over de informatiebeveiliging daarbij. Het systeem van Khonraad vormt daarbij een onderdeel van de door gemeenten gebruikte IV. Dus moeten gemeenten ook over het Khonraad systeem kunnen aangeven of en hoe het voldoende beveiligd is. Om ervoor te zorgen dat niet iedere gemeente dit afzonderlijk hoeft uit te zoeken met Khonraad is een informatief document opgesteld (zie bijlage). Dit document is opgesteld door de functionaris gegevensbescherming (FG) van Khonraad en is inhoudelijk beoordeeld door de CISO's van de gemeenten Den Bosch en Ede. Hun conclusies zijn:

1. Khonraad geeft op een afdoende manier invulling aan de eisen uit het 'Harmonisatiedocument informatiebeveiliging'.
2. Het opgestelde document beschrijft afdoende duidelijk hoe Khonraad invulling geeft aan de benoemde eisen.

Dit document kan nu door alle gemeenten gebruikt worden.

Vragen over dit document kunnen gesteld worden aan de FG van Khonraad, via fg@khonraad.nl.

4. FAQ over IV Wvggz

De voorbereidingen voor de Wvvgz zijn in volle gang. Er worden geregeld vragen gesteld over de IV die nodig is om de Wvggz uit te kunnen voeren, bijvoorbeeld over het Khonraad systeem en over het gebruik van veilige mail. Deze vragen nemen we op in een FAQ die binnen gemeenten verspreid kan worden. We zullen deze FAQ periodiek updaten. Zo krijgt iedere gemeente snel een overzicht van de gestelde vragen en beschikbare antwoorden. De eerste versie van de FAQ is als bijlage bij deze factsheet bijgevoegd.

5. Werkgroep IV Wvggz

De VNG coördineert een gemeentelijke werkgroep die zich met IV-vraagstukken rondom de Wvggz bezig houdt. Momenteel wordt aan deze IV-werkgroep deelgenomen door de gemeenten Utrecht, Den Bosch, Ede, Arnhem, Den Haag en BAR. Geïnteresseerden om deel te nemen aan deze werkgroep kunnen zich melden bij de projectsecretaris van het Wvggz-project bij de VNG, via info@VNG.NL.

Bijlage: Aan welke organisatorische eisen en randvoorwaarden moeten gemeenten voldoen?
De gemeente moet regels vaststellen (beleid) over hoe degenen die voor hem werken, gebruik mogen maken van geïmplementeerde communicatiemogelijkheden.

Er moeten ten minste regels worden vastgesteld over:
- het waarnemen van collega's tijdens diens afwezigheid;
- het mandateren en delegeren van toegang tot ad-hocberichten;
- de toegang tot informatie zonder een directe behandelrelatie (in zorginstellingen);
- de toegang tot functionele berichtenboxen (bijvoorbeeld orthopedie@voorbeeld.nl);
- het gebruik van een adresboek;
- het gebruik van functies die kunnen resulteren in het intrekken of wijzigen van ad-hocberichten;
- het gebruik van geautomatiseerde functies bij ontvangst van ad-hocberichten (waaronder maar niet uitsluitend, autoreply bij afwezigheid, leesbevestiging);
- bewaartermijnen;
- sleutelbeheer indien van toepassing, de mogelijkheden voor forensisch onderzoek (zie NEN 7510-2:2017, 16.1.1) en 'key escrow'-regeling;
- verantwoordelijkheden;
- verzendingsgronden;
- het continueren van de dienstverlening bij faillissement van de communicatiedienstenaanbieder;
- het informeren van de persoon over de veilige e-mailvoorziening.

KHONRAAD

Khonraad
Frequently Asked Questions
Wvggz

24 juni 2019, versie 1.0

Khonraad Software Engineering BV
Postbus 392
3740 AJ Baarn
Tel: 035 60 39 444
URL: www.khonraad.nl

Inleiding

Dit document bevat een overzicht van de aan Khonraad 'frequently asked questions' over de informatievoorziening (IV) die benodigd is voor de uitvoering van de Wvggz.

Voorbereiding op de Wvggz en de Wzd

Nr.	Onderwerp/vraag	Antwoord
1	Welke gegevens heeft Khonraad van mijn organisatie nodig?	Khonraad zal in de tweede helft van 2019 bij gemeenten, GGZ-instellingen en overige keten-partners informatie uitvragen die nodig is om het nieuwe Khonraad systeem te configureren.
2	Wanneer en door wie worden trainingen / instructies gegeven?	Khonraad maakt in het derde kwartaal van 2019 instructiemateriaal beschikbaar. De helpdesk van Khonraad is ook beschikbaar voor vragen van gebruikers.
3	(Vanaf wanneer) Is het mogelijk om te oefenen in de oefenomgeving van Khonraad.	Naar verwachting zal vanaf het vierde kwartaal van 2019 in de oefenomgeving geoefend kunnen worden met het nieuwe Khonraad systeem.
4	Wat wordt de naam van het nieuwe informatiesysteem?	Het systeem als geheel wordt voortaan aangeduid met de naam "Khonraad". Daarbij zal niet langer onderscheid worden gemaakt in verschillende productlijnen. De nieuwe faciliteiten zoals de ondersteuning van de crisismaatregel onder de Wvggz, de ondersteuning van het verkennend onderzoek onder de Wvggz, de ondersteuning van de inbewaringstelling onder de Wzd worden daarin integraal aangeboden.
5	Blijft de historie uit BOPZ-Online toegankelijk voor accounthouders?	De historie uit BOPZ-Online blijft - conform de wettelijke bewaartermijn - 5 jaar toegankelijk voor accounthouders.

Diensten Khonraad

Nr.	Onderwerp/vraag	Antwoord
1	Welke diensten levert Khonraad?	Khonraad levert de volgende diensten: a. Workflowmanagementsysteem ter ondersteuning van de uitvoering van de crisismaatregel en het verkennend onderzoek onder de Wvggz b. Workflowmanagementsysteem ter uitvoering van de inbewaringstelling onder de Wet zorg en dwang c. Berichtenbox d. Printservice e. Horen van betrokkene (overweging) f. Formulieren repository g. Ondersteuning bij het roosteren van de bereikbaarheid van bestuurders (piketroosters) h. Helpdesk i. Functioneel beheer
1a	Workflow managementsysteem Wvggz	Khonraad stelt een workflow managementsysteem als SAAS-oplossing beschikbaar aan gemeenten, GGZ instellingen en overige ketenpartners. Dit workflow managementsysteem ondersteunt de uitvoering van de crisismaatregel en verkennend onderzoek onder de Wvggz.
1b	Workflow managementsysteem Wzd	Khonraad stelt een workflow managementsysteem als SAAS-oplossing beschikbaar aan gemeenten. Dit workflow managementsysteem ondersteunt de uitvoering van de inbewaringstelling onder de Wzd.

1c	Berichtenbox	Een aansluiting hebben op Khonraad – en daarmee op de Berichtenbox – maakt het mogelijk te communiceren met het gemak van gewone e-mail, maar dan wel altijd **veilig**. De Berichtenbox is een onlosmakelijk onderdeel van de diensten die Khonraad al in de sector aanbiedt aan gemeenten, GGZ- VG- en PG-instellingen én daarmee gelieerde partijen zoals maatschappelijk dienstverleners, politie, Veilig Thuis en vele anderen. De Berichtenbox kent naast de bestaande functionele afzenders en bestemmingen (bijv. Bopz.IGJ@berichtenbox.nl) aan iedere professional een persoonlijk account toe. Het adresboek is daarmee altijd up-to-date én volledig. De Berichtenbox weigert (technisch) informatie te ontvangen van niet geauthentiseerde bronnen. Professionals met een Khonraad-account kunnen echter zonder beperkingen informatie uit welke bron dan ook (scans van documenten, e-mail van niet-veilige afzenders enz.) aan de voor hen toegankelijke dossiers toevoegen én verzenden naar anderen. Wanneer er informatie moet worden verstuurd aan niet-aangeslotenen – denk daarbij aan familievertegenwoordigers, curatoren, bewindvoerders, melders en natuurlijk de betrokkene zelf e.d. – kiest Khonraad met de Berichtenbox voor de weg van Veilige Mail. Daartoe staat een gateway naar een provider open, die op zijn beurt zorgt voor de veilige (o.a. met 2FA omgeven) aflevering. De gekozen transportweg wordt vooraf ingeregeld, afhankelijk van de keuze(s) die een organisatie (gemeente) voor een VM-leverancier heeft gemaakt. Op dit moment wordt de gateway al ingericht voor Zorgmail en Zivver. Met Cryptshare (die haar positie als VM-leverancier nog wil bepalen) wordt overlegd. Het streven is om te komen tot een open specificatie van de gateway, opdat sectorleden de ruimst mogelijke keuze blijven hebben uit de ongeveer dertig potentiële Veilig Mail aanbieders.

1d	Printservice	In een naar verwachting klein aantal gevallen, bijvoorbeeld omdat een organisatie niet tijdig – vóór 1 januari 2020 – een voorziening tot Veilige Mail heeft getroffen, of omdat een bestemming geen e-mail wenst of kan ontvangen, zal het nodig zijn per reguliere post te communiceren. Khonraad zal daarom de mogelijkheid bieden, vanuit het systeem een brief ter post aan te doen bieden. Deze remote afdruk zal in een blanco enveloppe worden aangeleverd aan Post-NL met een centraal retour adres. Van een dergelijke verzending, en eventueel bericht van afzender-retour, wordt uiteraard in het dossier aantekening gemaakt.
1e	Horen van betrokkene	Khonraad overweegt om een dienst in het leven te roepen, die 24x7 bereikbaar is en die betrokkene telefonisch kan horen namens de burgemeester. Van het horen zal een kort verslag worden gemaakt. Indien betrokkene hiermee instemt, zal er tevens een audio-opname worden gemaakt van het horen, die - desgewenst - kan worden afgeluisterd door de burgemeester.
1f	Formulieren repository	Voor de nog niet met uitgebreide workflow omgeven procedures, zoals de zorgmachtiging, zal in een (op de informatieproducten gebaseerde) formulieren repository worden voorzien. Daaruit kunnen (organisatie relevante) webformulieren worden ingevuld én ondertekend die via de Berichtenbox kunnen worden verstuurd.
1g	Piketroosters	De van Khonraad bekende ondersteuning van de piketdienst zal bij het nieuwe Khonraad-systeem gehandhaafd blijven.
1h	Helpdesk	Khonraad biedt - zoals u dat van ons gewend bent - een helpdesk die 24x7 bereikbaar is.
1i	Functioneel beheer	Khonraad voert het functioneel beheer uit van het Khonraad systeem, dat als SAAS-oplossing aan gemeenten, GGZ instellingen en overige ketenpartners beschikbaar wordt gesteld. Het aanvragen van accounts zal vergaand ondersteund worden door automatisering.

Informatiebeveiliging en certificering

Nr	Onderwerp/vraag	Antwoord
1	Is Khonraad ISO 27001 gecertificeerd en wat houdt dit in?	ISO/IEC 27001 is een wereldwijd erkende norm op het gebied van informatiebeveiliging. Khonraad is ISO27001/IEC 27001:2013 gecertificeerd.
2	Is Khonraad NEN7510 gecertificeerd en wat houdt dit in?	NEN7510 is een Nederlandse norm voor informatiebeveiliging voor de zorgsector. Khonraad is NEN7510-1:2017 gecertificeerd.
3	Wat is de scope van de Khonraad ISO27001 en NEN7510 certificering?	De huidige scope van de Khonraad SO27001/IEC 27001:2013 en NEN7510-1:2017 certificering luidt: "Het informatiebeveiligings management systeem omvat de ontwikkeling, verkoop en hosting van software-oplossingen BOPZ-Online, Huisverbod-Online en Berichtenbox." Deze scope zal in de loop van 2019 worden aangepast aan de ontwikkelingen rondom de Wvggz en de NTA7516:2019.
4	Kan ik de Verklaring van Toepasselijkheid ontvangen?	Khonraad heeft op basis van de resultaten van de risico-analyse alle beheersmaatregelen van de ISO27001/IEC 27001:2013 en vrijwel alle beheersmaatregelen van de NEN7510-1:2017 van toepassing verklaard. De bij de ISO27001/IEC 27001:2013 en NEN7510-1:2017 certificering behorende Verklaring van Toepasselijkheid kan desgewenst worden opgevraagd bij onze functionaris voor de gegevensbescherming.
5	Is Khonraad BIO compliant?	De Baseline Informatiebeveiliging Overheid (BIO) vervangt per 01-01-2020 de huidige BIG en BIR. Khonraad verwacht per 01-01-2020 BIO compliant te zijn en zal dit kunnen aantonen middels een in-control-statement. Certificering voor de BIO is niet mogelijk.
6	Is Khonraad NTA7516 compliant?	De NTA7516:2019 is de Nederlands Technische Afspraak voor de uitwisseling van ad-hoc berichten met persoonlijke gezondheidsinformatie. Khonraad verwacht per 01-01-2020 compliant te zijn met de voor Khonraad relevante onderdelen uit de NTA. Khonraad zal dit kunnen aantonen door middel van het opnemen van de relevante onderdelen van de NTA binnen de scope van het ISO27001/IEC 27001:2013 en NEN7510-1:2017 certificaat. Separate certificering voor de NTA7516:2019 is vooralsnog niet mogelijk.

7	Wat zijn de contactgegevens van de Functionaris voor de Gegevensbescherming van Khonraad?	Contactgegevens Functionaris voor de Gegevensbescherming Khonraad: Naam: drs. H. Bruns Telefoon: 035 6039444 E-mail: fg@khonraad.nl

Functionaliteit nieuwe Khonraad systeem

Nr	Onderwerp/vraag	Antwoord
1	Hebben we meerdere accounts nodig om de taken uit de verschillende wetten te kunnen uitvoeren?	Er is één account nodig om de taken uit de verschillen wetten uit te kunnen voeren. Een accounthouder kan in het nieuwe Khonraad systeem meerdere rollen hebben.
2	Blijft het één systeem of zijn het verschillende systemen?	Het blijft één systeem, zoals dat ook geldt voor het huidige BOPZ-Online en Huisverbod-Online.
3	Is het verschil goed zichtbaar? Weet een bestuurder voor welke wet hij een beslissing neemt?	Het zal voor de bestuurder duidelijk zijn voor welke wet een beslissing wordt genomen, zoals dat nu ook al het geval is voor de Wet Bopz en de Wet tijdelijk huisverbod.
4	Komt de communicatie via de besloten keten van de Berichtenbox ook in het dossier?	Omdat professionals in Khonraad samenwerken in elektronische dossiers, is het van belang dat de Berichtenbox-communicatie met anderen ook onderdeel uitmaakt van die dossiers. Daar wordt dan ook in voorzien. De (juridische) herleidbaarheid van de dossiervorming is daarmee optimaal.
5	Kunnen mails die (veilig) verstuurd worden in het kader van het verkennend onderzoek opgenomen worden in het dossier?	Omdat professionals in Khonraad samenwerken in elektronische dossiers, is het van belang dat de Berichtenbox-communicatie met anderen (al dan niet met gebruikmaking van veilige mail) ook onderdeel uitmaakt van die dossiers. Daar wordt dan ook in voorzien. De (juridische) herleidbaarheid van de dossiervorming is daarmee optimaal.
6	Kunnen er documenten worden toegevoegd aan het dossier?	Er komt een mogelijkheid om documenten en media toe te voegen aan het dossier.

Koppelingen met andere systemen

Nr	Onderwerp/vraag	Antwoord
1	Komt er een koppeling met de GBA; worden gegevens geverifieerd d.m.v. BSN?	Het gebruik van het BSN bij gegevensverwerking en -verstrekking binnen de Wvggz-keten wordt door alle betrokken partijen zeer wenselijk geacht. In tegenstelling tot bijvoorbeeld in de Jeugdwet, is dit echter niet expliciet voorgeschreven en/of geregeld in de Wvggz. Dit roept de vraag op of en in hoeverre partijen het BSN mogen verwerken bij de uitvoering van hun taken en de uitwisseling van gegevens in het kader van de Wvggz. Momenteel worden gesprekken gevoerd met het beleidsdepartement om hierover duidelijkheid te verschaffen. De resultaten hiervan worden afgewacht.
2	Welke systeemkoppelingen komen er?	Vanuit de Wvggz en Wzd is een aantal werkprocessen voorzien die uitgebreide workflow en casemanagement ondersteuning hebben: • de crisismaatregel; • het verkennend onderzoek; • de inbewaringstelling. De systeem-meldingen die vanuit deze workflows zijn voorzien, vinden alle via systeemkoppelingen plaats. Daartoe is een systeemkoppeling voorzien met het/de OM, IGJ, PvP, RvR en CIZ.

Autorisatie

Nr	Onderwerp/vraag	Antwoord
1	Kunnen 'externe' partijen, zoals de GGD of GI, ook geautoriseerd worden om stappen uit het werkproces uit te voeren in het CM-systeem?	Dat is mogelijk. Verwerkingsverantwoordelijke bepaalt welke partijen / actoren geautoriseerd moeten worden voor de verschillende stappen in het werkproces. Khonraad richt op basis daarvan de werkprocessen in.
2	Is het autorisatiemodel van de werkprocessen op generieke rollen ingericht?	De toegang tot het Khonraad systeem wordt verleend wordt verleend op basis van een authenticatie- en autorisatiemodel. Hierin heeft Khonraad generieke autorisatierollen vastgelegd, waaraan rechten zijn gekoppeld.

Kosten Khonraad dienstverlening

Nr	Onderwerp/vraag	Antwoord
1	Wat zijn de kosten van het Khonraad systeem?	De inrichting van de werkprocessen zal voor de betrokken ketenpartners in de betreffende gemeente of regio plaatsvinden. Na afstemming daarover zal Khonraad contractanten een passende aanbieding kunnen doen. Als gevolg van de integratie van de voormalige productlijnen zal daarbij tevens een wijziging in de tarievenstructuur worden toegepast.

KHONRAAD

Harmonisatie maatregelen informatiebeveiliging Wvggz

24 juni 2019, versie 1.0

Khonraad Software Engineering BV
Postbus 392
3740 AJ Baarn
Tel: 035 60 39 444
URL: www.khonraad.nl

Inhoudsopgave

1 Inleiding

Dit document beschrijft de wijze waarop door Khonraad Software Engineering invulling gegeven wordt aan het document "Harmonisatie maatregelen informatiebeveiliging Wvggz" v 1.0, dat op 12 december 2018 is vastgesteld door de Bestuurlijke Keten Raad (BKR).

In dit document is de indeling van het harmonisatiedocument gevolgd, zodat beide documenten eenvoudig naast elkaar gelegd kunnen worden.

Khonraad vindt het belangrijk om zoveel mogelijk bij te dragen aan het veilig(er) maken van de communicatie in de bestuurlijke en aanhangige domeinen.

2 Principes voor informatiebeveiliging samenwerking Wvggz

2.1 Organisaties zijn zelf verantwoordelijk voor informatiebeveiliging en privacy en stemmen af in ketenverband

Akkoord, geen vragen of opmerkingen.

2.2 Afspraken gaan eerst over informatieverstrekking tussen mensen in hun organisatorische rol binnen de Wvggz, afspraken over informatie- en communicatiemiddelen zijn een afgeleide daarvan

Akkoord, geen vragen of opmerkingen.

2.3 Informatiebeveiliging wordt situationeel afgewogen tegen andere risico's

Akkoord, geen vragen of opmerkingen.

2.4 De informatiebeveiliging gaat uit van een federatieve benadering

Akkoord, geen vragen of opmerkingen.

2.5 Organisaties maken onderling afspraken over gegevensverwerking en maken zelf afspraken met hun eigen gegevensverwerkers

Aangezien Khonraad de centrale verwerker is voor alle organisaties die gebruik maken van het CM-systeem en de VO-module en er sprake is van een ketenworkflowmanagement systeem, verdient het de sterke voorkeur om een generieke verwerkersovereenkomst op te stellen. De verwerkersovereenkomst van de VNG als leidend nemen is een wens van de gemeenten. De overeenkomst van Khonraad is daarmee in lijn en op punten nader uitgewerkt.

2.6 Afspraken over compliance hergebruiken bestaande compliance eisen en processen

Akkoord, geen vragen of opmerkingen.

2.7 Van elke verstrekking is exact afgesproken op welk moment de verwerking van de ontvanger start

Afgesproken is om privacy rollen en verantwoordelijkheden in de keten in kaart te brengen in een referentie-DPIA, waarbij zowel de GGZ- als de gemeentelijke sector betrokken zijn. Er wordt op dit moment gewerkt aan een document met verwerkingsgrondslagen. GGZ Nederland en de VNG leveren vragenlijsten aan, op basis waarvan Khonraad input kan leveren voor de DPIA.

2.8 Verwerking van ontvangen informatie is altijd tot een natuurlijk persoon traceerbaar

Inzien en wijzigen van gegevens door natuurlijke personen wordt gelogd. Deze logging wordt in het CM-systeem en de VO-module ingericht conform NEN7513 en op verzoek beschikbaar gesteld aan (vertegenwoordiger van) bestuurders. Hiervoor wordt een nieuwe rol aangemaakt.

2.9 De organisaties hebben aantoonbaar hun (bedrijfs)proces en informatie geclassificeerd voordat informatie gedeeld wordt met ketenpartners

Akkoord. Zie hoofdstuk 4 (Classificeren en authenticeren) voor een nadere toelichting.

3 Geldende normenkaders

Khonraad Software Engineering B.V. is ISO/IEC 27001:201 en NEN 7510-1:2017 gecertificeerd. Aangezien de BIG en de BIR per 2020 worden vervangen door de BIO, heeft Khonraad er voor gekozen om dit compliance traject uit te stellen. Het streven van Khonraad is om per 1 januari 2020 te voldoen aan de BIO norm. Khonraad brengt op dit moment in kaart wat hiervoor nodig is en of het haalbaar is om vanaf 1 januari 2020 aan deze norm te voldoen.

4 Classificeren en authenticeren

Een samenvatting van de dataclassificatie door Khonraad luidt:

Classification	Description	Examples	Treatment
Public	Information of this kind can be freely distributed to anyone.	• Information on our public web site • Brochures and leaflets	No special measures need to be taken to protect this information.
Internal	Information of this kind is meant to be kept internally, but no harm would be done if it would fall into wrong hands. This information can be shared with team members or external parties when deemed necessary.	• Policies and Procedures • Assets	Although email communication is not deemed secure, it is OK to transfer information labelled "Internal".Information is classified as "Internal" unless stated otherwise.
Confidential	Information of this kind is meant to be handled with special care. It should not be left unattended	• Financial information • Data in CRM and HR systems • All Personally Identifiable Information	Confidential information must be transferred with proper protection.

Sensitive	Information of this kind requires special protection. Theft or loss should be reported with the authorities.	• Healthcare information • Special categories of personal information ("bijzondere persoons-gegevens")	As Confidential, enhanced with: • Authentication secured with 2FA • TLS encryption • No read access by own/maintenance personnel • Auditing/logging

Alle gegevens in BOPZ-Online (vanaf 2020: CM-systeem) vallen in de hoogste klasse "Sensitive". Binnen deze klasse zullen minimaal twee subklassen worden gedefinieerd, aangezien differentiatie in dataclassificatie binnen het CM-systeem van belang wordt geacht. Deze subklassen zullen worden meegegeven als annotatie in het datamodel.

Accounts zijn persoonsgebonden en de toegang is beperkt door middel van een twee-factor-authenticatie mechanisme.

5 Vereiste beveiligingsniveau informatie Wvggz

Van toepassing op het CM-systeem en de VO-module zijn informatiestroom 1 t/m 7, 9, 10, 14, 17, 22, 27 en 28.
Niet van toepassing zijn informatiestroom: 8, 11 t/m 13, 15 en 16, 18 t/m 21, 23 t/m 26 en 29 t/m 31.

Zorgaanbieders (opnamelocaties of ambulant) vallen onder GGZ (informatiestroom 7).
RvR valt onder overige betrokkenen (informatiestroom 8).

6 Geharmoniseerde maatregelen

6.1 Authenticatie en identificatie organisaties

6.1.1 (1) De volgende organisaties worden in het licht van deze afspraken erkend als organisaties die vanuit hun wettelijke rol informatie uitwisselen in het kader van de Wvggz: het Openbaar Ministerie (OM), alle rechtbanken, de Hoge Raad, alle gemeenten, de Nationale Politie, de stichting PvP, de landelijke stichting Familievertrouwenspersonen (LSFVP), de Raad voor Rechtsbijstand (RvR).

De IGJ ontbreekt.

6.1.2 (2) Zorgaanbieders zijn rechtspersonen en worden in het licht van deze afspraken erkend als organisaties die vanuit hun wettelijke rol informatie uitwisselen in het kader van de Wvggz, zolang ze correct geregistreerd staan in het openbaar register conform atikel 1:2 Wvggz

Het openbaar register komt er wel, maar dit register kan 'achter lopen'. Daarom zal de situatie blijven zoals deze nu is. Er zal dus een eigen register worden bijgehouden door Khonraad. Dit zal initieel worden gevuld vanuit BOPZ-Online. Digitale koppeling of controle vanuit Khonraad tegen het openbare register zal (vooralsnog) niet mogelijk zijn.

6.2 Authenticatie bij toegang

6.2.1 (3) Authenticatie van personen voor het toegang krijgen tot gegevens geschiedt op het niveau eHerkenning - niveau 3 / eIDAS substantieel.

6.2.1.1 Inlogmethode

Accounts zijn persoonsgebonden. Er wordt ingelogd met gebruikersnaam en pincode, aangevuld met een SMS-code (tweede factor). Khonraad is niet voornemens om hier op korte termijn iets in te veranderen (TOTP of anderszins). Een aanvulling met What's app business wordt overwogen.

6.2.1.2 Aanvraagprocedure

Khonraad verstuurt blanco accountformulieren als pdf bij voorkeur aan accounthouders of contactpersonen. Als een beller (nog) geen accounthouder of contactpersoon is, verwijzen we hem of haar bij voorkeur naar de accountbeheerder van de betreffende organisatie of naar een bestaande accounthouder. Uitzonderingen daarop zijn mogelijk, mits middels e-mailadres en/of telefoonnummer is vastgesteld dat de beller daadwerkelijk werkzaam is bij de organisatie waarvoor het account wordt aangevraagd.
Het ondertekende accountaanvraagformulier wordt door de klant per post of per veilige e-mail naar Khonraad verstuurd. De ambitie is om de accountaanvragen in de toekomst volledig te digitaliseren.

6.2.1.3 Controle bevoegdheid tijdens aanvraagproces

Accounts kunnen alleen worden aangemaakt bij een organisatie die klant is bij BOPZ- of Huisverbod-Online. Sommige klanten vormen samen één organisatie. Aan de hand van het werkadres, het (algemene) telefoonnummer, de autorisator of de aanvrager kan vrijwel altijd worden vastgesteld bij welke klant de account zal moeten worden aangemaakt. Bij twijfel wordt contact opgenomen met de aanvrager of de autorisator.

De accountaanvraag dient te zijn geautoriseerd door de accountbeheerder van de aanvragende organisatie of een andere bekende contactpersoon of accounthouder. Controle van de persoonsgegevens is de verantwoordelijkheid van de organisatie die het account aanvraagt. De helpdesk van Khonraad controleert de volledigheid en leesbaarheid van de aanvraag, controleert de rol en checkt of een dergelijk account reeds bestaat.
Daarna wordt het account aangemaakt en - afhankelijk van de rol - voorzien van digitale handtekening. In het geval van een bestuurder wordt op de website van de gemeente gecontroleerd of de betreffende gebruiker inderdaad wordt genoemd als bestuurder en wordt de piketvolgorde en het piketttelefoonnummer geregistreerd.
De ervaring heeft geleerd dat koppeling met de KvK geen toegevoegde waarde heeft. Een dergelijke koppeling zal niet worden gerealiseerd.
De controlevragen blijven gehandhaafd. Gekeken zal worden hoe er strengere eisen aan de controlevragen kunnen worden gesteld en de mogelijkheid van een signaal achteraf wordt overwogen.

6.2.1.4 Uitgifte van het middel

De gebruikersnaam wordt per e-mail verstuurd. Gebruikers wordt verzocht om te bellen naar de Khonraad helpdesk. Nadat de helpdesk de identiteit van de gebruiker heeft gecontroleerd door middel van de controlevraag, ontvangt de gebruiker telefonisch een tijdelijke pincode. Hiermee kan hij/zij éénmalig inloggen. Direct na het inloggen wordt de gebruiker gevraagd om een persoonlijke pincode te kiezen. Deze is bij niemand anders bekend dan bij de gebruiker zelf. De SMS-code (tweede factor) die benodigd is om in te kunnen loggen, ontvangt de gebruiker op zijn/haar mobiele nummer. Wanneer er problemen zijn met de ontvangst van de SMS-code, dan kan de Khonraad-helpdesk een SMS-code verstrekken, nadat de identiteit van de gebruiker is gecontroleerd aan de hand van de controlevraag.

6.2.1.5 Foutieve inlog of onrechtmatig gebruik

Wanneer men driemaal probeert in te loggen met een verkeerde combinatie van gebruikersnaam en pincode, wordt het account direct geblokkeerd. Om het account te deblokkeren moet contact worden gelegd met de helpdesk, die aan de hand van de controlevraag de identiteit van de gebruiker controleert en alleen dan het account weer vrijgeeft. De gebruiker dient dan wel weer zelf een nieuwe pincode te kiezen.
Indien de helpdesk van Khonraad constateert dat er sprake is van oneigenlijk gebruik van een account, dan wordt dit direct intern gemeld aan de achterwacht. Als het vermoeden bestaat dat er sprake is van niet-valide of onrechtmatig gebruik, kan de achterwacht er voor kiezen om de account te blokkeren, en/of de pincode te veranderen. Pas na persoonlijk contact van de helpdesk of achterwacht met de accounthouder, waarbij de accounthouder nadrukkelijk wordt gewezen op het persoonlijke karakter van de accounts, wordt het account onder condities weer vrijgegeven.

6.2.2 (4) Het middel voor authenticatie om personen namens een rechtspersoon toegang te geven tot gegevens is eHerkenning, indien mogelijk.
De geschetste invulling is aan te merken als e-Herkenning, niveau 2+. Er is geen sprake van fysieke identificatie met vertoning van een origineel identiteitsbewijs (e-Herkenning niveau 3). E-Herkenning niveau 2+ wordt afdoende geacht, gezien extra waarborgen in context en werkproces en urgentie in het werkproces.

6.2.3 (5) Medewerkers toegang geven tot gegevens mag ingericht worden met single sign-on mits gebaseerd op SAML en wordt aangevuld met twee-factor authenticatie
Single sign-on wordt niet toegepast.

6.2.4 (6) Tussen partijen worden afspraken gemaakt over de wijze van identificatie van communicerende entiteiten. Waar mogelijk en nuttig wordt afgesproken bestaande landelijke registers te gebruiken (Basisregistratie Personen (BRP), Handelsregister (HR), Beroepen in de Individuele Gezondheidszorg (BIG), AGB-register). Waar mogelijk worden afspraken gemaakt over vertrouwde identiteitsbronnen.
Koppeling Handelsregister wordt niet zinvol geacht (zie paragraaf 6.2.1.3). Koppeling met openbaar register is vooralsnog niet mogelijk (zie paragraaf 6.1.2). Koppeling met BIG- en AGB-register wordt niet zinvol geacht. Koppeling met de BRP is wenselijk.

6.3 Digitaal transport

6.3.1 (7) Communicatie over niet-vertrouwde netwerken (o.a. internet) verloopt alleen via beveiligde verbindingen (voor alle vormen van digitale communicatie o.a. berichten, e-mail en website toegang).
Het toegangsportal van Khonraad op www.khonraad.nl maakt gebruik van een TLS-verbinding, de standaard voor de encryptie van internetverbindingen, waarbinnen alle gegevens uitsluitend versleuteld worden verstuurd. Khonraad heeft TLS geconfigureerd volgens de meest recente beveiligingsrichtlijnen van het Nationaal Cyber Security Centrum (NCSC); uitsluitend configuraties met de status 'goed' worden gebruikt. Voor de koppeling met het OM wordt tweezijdig TLS gebruikt. Dit betekent dat niet alleen de client het bewijs van identiteit van de server controleert, in de vorm van een digitaal certificaat, maar dat de server op zijn beurt ook een digitaal certificaat vraagt aan de client, zodat zowel server als client weten met wie zij communiceren.
Berichten worden verzonden middels de Berichtenbox, een virtueel veilig communicatieplatform. Op de Berichtenbox aangesloten organisaties kunnen (uitsluitend) aan elkaar berichten zenden; het is niet mogelijk om buiten de keten te communiceren. Daarnaast zal interoperabiliteit met andere veilig e-mail oplossingen (bijvoorbeeld Zivver en Zorgmail) worden gerealiseerd.

6.3.2 (8) Beveiligde verbindingen worden gerealiseerd op basis van authenticatie van de betreffende organisatie met minimaal een middel op het niveau eIDAS substantieel.
Voor alle gebruikers wordt een zelf gekozen controlevraag toegepast.
Verder geen vragen of opmerkingen.

6.3.3 (9) De besloten netwerken Justitienet (van justitie: Openbaar Ministerie, rechtspraak) en Politienet (Nationale Politie) en GGI-Netwerk (gemeenten) gelden als vertrouwde netwerken.
Duidelijk. Geen vragen of opmerkingen.

6.4 Toegangsautorisatie

Khonraad maakt geen gebruik van deze faciliteiten, behoudens toegang tot het OM-netwerk via Justid.

6.5 Autorisatie

6.5.1 (13) Iedere organisatie heeft een formele aanvraag-, goedkeurings- en intrekkingsprocedure voor toewijzing en intrekking van toegangsrechten, incl. logging daarvan
Het is de verantwoordelijkheid van onze klanten om te beschikken over een formele aanvraag-, goedkeurings- en intrekkingsprocedure voor toewijzing en intrekking van toegangsrechten. Het moet altijd helder zijn wie de contactpersoon voor autorisatie is. Dit wordt een aparte rol (accountbeheerder). Gemeenten kunnen via de rol accountbeheerder de interne procedure voor accounts checken.
Verzoeken komen telefonisch of per veilige e-mail bij Khonraad binnen en worden door Khonraad geregistreerd. Datzelfde geldt voor de start- en einddatum van het account. Ambitie is volledige digitalisering van de accountaanvragen.
Wijzigingen in accounts worden gelogd. Deze logging is momenteel niet beschikbaar voor klanten. De logging zal worden uitgebreid, met casus gerelateerde toegang.

6.5.2 (14) Groepsaccounts zijn toegestaan in deze processen. Uitgezonderd specifieke gegevens die alleen op combinatie van persoon en casus toegankelijk mogen zijn.
Voor alle gegevens binnen het CM-systeem en de VO-module geldt dat deze uitsluitend op combinatie van persoon en casus toegankelijk mogen zijn. Derhalve zijn groepsaccounts niet toegestaan.

6.5.3 (15) Toegang kan casus gerelateerd zijn op basis van in het proces bepaalde betrokkenheid op aangeven van een communicatiepartij.
Voor medewerkers van zorginstellingen is toegang tot gegevens in gedigitaliseerde patiëntendossiers alleen rechtmatig indien en voor zover een medewerker rechtstreeks betrokken is bij de behandeling van, zorgverlening aan of beheersmatige afwikkeling van die zorgverlening (o.a. artikel 7:457, eerste en tweede lid Burgerlijk Wetboek en NEN7510). Toegang is dus casus gerelateerd.
Dit betekent dat we zullen moeten autoriseren na vaststelling van rechtstreekse betrokkenheid. In de praktijk betekent dit dat de psychiater zal moeten verklaren dat er sprake is van rechtstreekse betrokkenheid, alvorens hij/zij een evt. bestaand dossier van betrokkene kan inzien. Het zoeken naar bestaande dossiers zal zodanig moeten worden ingericht, dat uitsluitend het exact matchende zoekresultaat wordt getoond.

6.6 Beschikbaarheid

6.6.1 (16) In ketenwerkprocessen met de beschikbaarheidsclassificatie "Essentieel" is de procesbeschikbaarheid gegarandeerd met een maximale uitval van 30 minuten, met een maximum van 2 keer uitval per maand.
Khonraad voldoet ruimschoots aan deze eis.

6.6.2 (17) In ketenwerkprocessen met de beschikbaarheidsclassificatie "Noodzakelijk" is de procesbeschikbaarheid gegarandeerd met een maximale uitval van 60 minuten gedurende kantoortijden, met een maximum van 2 keer uitval per maand.
Is niet van toepassing op het CM-systeem, wel op de VO-module. Historische cijfers laten zien dat zelfs aan de beschikbaarheidsclassificatie "Essentieel" ruimschoots wordt voldaan.

6.7 Logging

6.7.1 (18) Partijen geven elkaar op verzoek binnen twee weken inzage in logging.
Logging wordt gedefinieerd (op basis van NEN7513) en klanten krijgen op verzoek inzage in deze logging.

6.8 Mobiele apparatuur

6.8.1 (19) Voor mobiele apparaten geldt het Zero-footprint-concept
Het CM-systeem en de VO-module zijn Saas-applicaties. Daarmee is voor wat betreft de verantwoordelijkheid van Khonraad aan dit uitgangspunt voldaan.

6.8.2 (20) Verplichte beveiliging en op afstand wissen
Voor de eigen mobiele apparatuur heeft Khonraad dit geregeld conform ISO27001 en NEN7510.