Bijlage B: Toelichting beveiliging, Security Monitoring en toetsing behandelrelatie

De koepels hebben in overleg met Nictiz een doorstartmodel 1.0 opgesteld op basis waarvan de dienstverlening van het landelijk schakelpunt voortgezet kan worden in een Servicecentrum Zorgcommunicatie (SZC). Dit model is voorgelegd aan het College Bescherming Persoonsgegevens (CBP) ten behoeve van een bespreking op 24 november 2011.

Onderhavig document geeft een nadere toelichting op de beveiliging in de doorstartsituatie. Specifiek besproken wordt controle en het toezicht op rechtmatige toegang tot de gegevens door middel van security monitoring en het toetsen van de behandelrelatie in het autorisatieproces.

1. Beveiliging in de doorstart

Deze paragraaf bespreekt de waarborgen rondom informatiebeveiliging binnen 'AORTA'. AORTA[1] is de infrastructuur van de landelijke gegevensuitwisseling. De AORTA informatie is openbaar beschikbaar via de Nictiz website[2]. Dit bevat een beschrijving van de onderdelen van AORTA. De waarborgen zien op de toegang tot de informatie in het goed Beheerde Zorgsysteem (GBZ)[3] en het transport van informatie tussen het GBZ en het landelijk schakelpunt via de zorgserviceprovider (ZSP)[4].

De Nederlandse normen voor informatiebeveiliging in de zorg, ook wel aangeduid als de 'NEN-normen' vormen de basis voor de maatregelen in het kader van informatiebeveiliging voor ieder onderdeel van AORTA. Het betreft de NEN 7510/7511 normen en de in de subnormen NEN 7512 en NEN 7513 vastgelegde normen. De gereviseerde NEN 7510-11 zal in een nieuwe release worden doorgevoerd zover van belang.

Vertrouwelijkheid

Binnen AORTA zijn diverse maatregelen getroffen die waarborgen dat patiëntgegevens vertrouwelijk blijven en niet toegankelijk worden voor onbevoegde partijen. In de eerste plaats waarborgt het landelijk schakelpunt door middel van de UZI-pas en andere beveiligingscertificaten van het UZI-register dat gegevens slechts kunnen worden opgevraagd of verstuurd vanuit gekwalificeerde zorgsystemen en enkel door personen waarvan de identiteit is vastgesteld en gevalideerd.

In de tweede plaats worden de gegevens die tussen een GBZ en het landelijk schakelpunt worden uitgewisseld tijdens het transport versleuteld. Zodoende kunnen onbevoegden de gegevens niet inzien of wijzigen. De beveiligingscertificaten die hiervoor nodig zijn worden uitgegeven door het UZI-register. Het netwerk van de ZSP is overigens een besloten netwerk en geen onderdeel van het internet.

Om patiëntgegevens te mogen aanmelden bij of opvragen via het landelijk schakelpunt dient een zorgaanbieder over de juiste toegangsrechten te beschikken. De concrete toegangsrechten van een zorgaanbieder hangen samen met de rolcode die is geregistreerd op de UZI-pas. Rolcodes komen overeen met beroepstitels in het BIG-register (zie de passage over het UZI-register in de bijlage).

---

1 Nictiz; "Architectuur AORTA"; versie 6.10.0.0; Den Haag, 12 oktober 2011; gepubliceerd op http://www.nictiz.nl/uploaded/FILES/html_cabinet/live/Infra/Gedeeld/AORTA_Arch_Architectuur_AORTA.htm

2 Zie ook het volledige documentatie-overzicht op http://www.nictiz.nl/page/Infrastructuur/AORTA-documentatie/AORTA-documentatie-2011

3 Nictiz; *"Programma van eisen organisatie goed beheerd systeem (GBx) – AORTA 2011"*; versie 6.10.0.0; Den Haag, 12 oktober 2011; gepubliceerd op http://www.nictiz.nl/uploaded/FILES/html_cabinet/live/Infra/Gedeeld/AORTA_GBx_PvE_Organisatie.htm

4 Nictiz; *"Programma van eisen zorgserviceprovider (ZSP) – AORTA 2011"*; versie 6.10.0.0; Den Haag 12 oktober 2011, gepubliceerd op http://www.nictiz.nl/uploaded/FILES/html_cabinet/live/Infra/Gedeeld/AORTA_ZSP_PvE_ZorgServiceProvider.htm

Integriteit

Om ervoor te zorgen dat zorgaanbieders elkaar voorzien van volledige en correcte informatie, zijn binnen AORTA verschillende maatregelen getroffen. In de eerste plaats wordt tijdens het kwalificatietraject van een goed beheerd zorgsysteem (GBZ) getoetst of gegevens die worden verstuurd op de juiste wijze worden gecodeerd.

In de tweede plaats vindt ook tijdens de daadwerkelijke uitwisseling een validatie plaats. Er wordt daarbij onderscheid gemaakt tussen twee situaties:

1. van gegevens die in het landelijk schakelpunt zelf worden verwerkt en opgeslagen (bijvoorbeeld verwijsindexgegevens) wordt gecontroleerd of het bericht correct is ontvangen;

2. van gegevens die door het landelijk schakelpunt slechts worden doorgestuurd naar een GBZ controleert het landelijk schakelpunt slechts de 'envelop' waarin de gegevens zijn verpakt.

Fouten die het landelijk schakelpunt constateert worden geregistreerd in de centrale logging, zodat passende maatregelen kunnen worden genomen.

Tijdens het transport wordt de integriteit van gegevens beschermd door het versleutelen van de verbinding, alsmede door versleuteling van enkele voor het bericht kenmerkende gegevens in het bericht zelf.

Beschikbaarheid

De beschikbaarheid van de landelijke infrastructuur als geheel wordt gegarandeerd door middel van een aantal eisen ten aanzien van goed Beheerde Zorgsystemen (GBZ'en), AORTA en het landelijk schakelpunt.

In de eerste plaats is de productieomgeving van het landelijk schakelpunt het hele jaar door, vierentwintig uur per dag, zeven dagen per week, opengesteld voor gebruik. Ook de op AORTA aangesloten ZSP's (Zorg Serviceproviders, oftewel netwerkleveranciers) en GBZ'en voldoen aan deze beschikbaarheidseis om opgevraagde patiëntgegevens te kunnen aanleveren.

In de tweede plaats is het landelijk schakelpunt redundant uitgevoerd. Dat wil zeggen dat de productieomgeving van het landelijk schakelpunt verspreid is over twee geografische locaties die voldoen aan de hoogste beveiligings- en continuïteitseisen. Daarmee wordt een beschikbaarheidspercentage van >99,98% geboden.

De ZSP's hebben hun infrastructuur zodanig ingericht dat de faalkans en de hersteltijd van (netwerk-)componenten in overeenstemming zijn met bovenstaande eisen. De ZSP maakt daarbij gebruik van redundantie in het netwerk om single points of failure te voorkomen.

Om verstoring van de operationele omgeving door testen te voorkomen beschikt het landelijk schakelpunt, naast de operationele ICT-omgeving, over:

- Een ontwikkelomgeving voor de ontwikkeling van nieuwe functies van het landelijk schakelpunt;

- Een testomgeving waarin technische tests worden uitgevoerd;

- Een acceptatieomgeving, waarin de uiteindelijke acceptatie van het landelijk schakelpunt en de kwalificatie van Goed Beheerde Zorgsystemen plaats kan vinden.

In de derde plaats beschikt het landelijk schakelpunt over procedures om opgeslagen gegevens veilig te stellen en in voorkomende gevallen te herstellen. Dagelijks wordt een back-up gemaakt van de gegevens die zijn opgeslagen in het operationele landelijk schakelpunt. De back-up wordt binnen 24 uur overgebracht naar een locatie, waar het is beschermd tegen beschadiging en onbevoegde inzage. Herstelprocedures worden jaarlijks of na het aanbrengen van wijzigingen in het landelijk schakelpunt getest.

Ook GBZ'en dienen dagelijks een back-up van de lokaal opgeslagen gegevens te maken conform de eisen.

Ten slotte wordt de belasting van het landelijk schakelpunt bijgehouden. Deze wordt uitgedrukt in het aantal partijen dat hierop is aangesloten en in de hoeveelheid gegevens die wordt uitgewisseld. Het landelijk schakelpunt is schaalbaar ontworpen zodat het mogelijk is om naar behoefte de capaciteit ervan uit te breiden, bijvoorbeeld door toevoeging van hardwarecomponenten.

Onweerlegbaarheid

AORTA biedt faciliteiten om het bericht zonodig te voorzien van een elektronische handtekening om de onweerlegbaarheid van de gegevens te garanderen[5].

---

[5] Nictiz; *"Implementatiehandleiding elektronische handtekening met UZI-pas – AORTA 2011"*; versie 6.10.0.0; Den Haag, 12 oktober 2011; gepubliceerd op http://www.nictiz.nl/uploaded/FILES/html_cabinet/live/Infra/Authenticatie/AORTA_Auth_Sig_IH_Elektronische_handtekening_UZI.htm

Van gegevens die worden ontvangen en verzonden door het landelijk schakelpunt wordt in een centrale logging (gebruiksregistratie) onder meer bijgehouden welke zorgaanbieder wanneer en welk type patiëntgegevens opvraagt of verstuurt.

De centrale gebruiksregistratie ('logging') zorgt ervoor dat eventueel misbruik van privileges achteraf kan worden vastgesteld en passende maatregelen kunnen worden getroffen.

Landelijk schakelpunt

Deze paragraaf beschrijft de eisen die zijn gesteld om de kwaliteit en beveiliging van het landelijk schakelpunt te waarborgen. Deze eisen zijn opgenomen in het Programma van Eisen landelijk schakelpunt (PvE Zorginformatiemakelaar). Zie verder ook de bijlage Normering informatiebeveiliging Landelijk EPD.

Beveiligingsbeleid

Voor het landelijk schakelpunt is een beveiligingsplan opgesteld. Het beveiligingsplan specificeert een stelsel van beveiligingsmaatregelen en -procedures. De beheerder van het landelijk schakelpunt is verantwoordelijkheid voor de implementatie en handhaving van deze maatregelen en procedures.

Organisatieplan

Voor het landelijk schakelpunt is een organisatieplan opgesteld waarin de verantwoordelijkheden ten aanzien van beveiliging zijn beschreven. Het organisatieplan omvat onder meer informatie over de organisatiestructuur, personeelsbeleid, huisvesting

en een opleidingsplan. Het geheel van processen, procedures en werkinstructies ten behoeve van de dienstverlening van het landelijk schakelpunt is vastgelegd in een dossier afspraken en procedures. Over verrichte werkzaamheden wordt periodiek gerapporteerd.

Operationeel beheer

Beheer van de ICT-systemen betreft de instelling van systeemparameters, het operationeel houden van het landelijk schakelpunt, bewaking van aangesloten goed Beheerde Zorgsystemen, het oplossen van technische problemen en aansluiting van zorgserviceproviders (ZSP's) en goed beheerde zorgsystemen (GBZ'en).

Bij beheer van autorisaties gaat het om de configuratie van de toegangsrechten die horen bij specifieke beroepstitels, zoals vastgelegd in het autorisatieprotocol. Tevens dienen eventuele uitsluitingen die een patiënt aangeeft te worden doorgevoerd in het autorisatieprofiel van de betreffende patiënt.

Om beveiligingsredenen worden het beheer van autorisaties, het beheer van de centrale gebruiksregistratie en het beheer van de ICT-systemen door verschillende personen uitgevoerd. De beheerfuncties van het landelijk schakelpunt zijn slechts toegankelijk voor aangewezen personen.

Eisen ten aanzien van personeel

Medewerkers van het landelijk schakelpunt beschikken over de vakkennis, ervaring en kwalificaties die noodzakelijk zijn voor de werkzaamheden die zij vervullen. Personeel dat betrokken is bij gegevensverwerkende taken heeft een geheimhoudingsplicht en dient te beschikken over een Verklaring Omtrent het Gedrag (VOG). Tijdelijke medewerkers hebben geen toegang tot persoonsgegevens. Bij beëindiging van de relatie met de werknemer worden diens toegangsrechten ingetrokken.

Fysieke beveiliging

De ICT-infrastructuur van het landelijk schakelpunt bevindt zich in een fysiek beveiligde omgeving en is slechts toegankelijk voor geautoriseerd personeel. Derden mogen de gebouwen slechts betreden onder begeleiding van geautoriseerd personeel.

Apparatuur in het landelijk schakelpunt is zodanig geplaatst en beveiligd dat de risico's van schade en storing van buitenaf en de kansen op ongeautoriseerde toegang minimaal is.

Bescherming tegen indringers

Het landelijk schakelpunt wordt beschermd tegen elektronische indringers, door middel van 'intrusion detection' en 'intrusion prevention'. Daarnaast worden regulier indringerstesten uitgevoerd en is voorzien in procedures voor de afhandeling van beveiligingsincidenten. Vermoedens van onrechtmatig gebruik worden gemeld aan de toezichthouders.

Naleving en beveiligingsincidenten

Ten behoeve van de controle op de juiste werking en naleving van de juiste procedures worden alle beheerhandelingen vastgelegd in een logboek. Periodiek, of wanneer daar aanleiding toe is, kan een audit op het landelijk schakelpunt worden uitgevoerd.

Op elk moment kan worden gecontroleerd of de beveiliging van de locatie van het landelijk schakelpunt aan de eisen voldoet. Het beveiligingsplan wordt jaarlijks door een onafhankelijke partij beoordeeld.

Zorgserviceprovider (ZSP)

Een zorgserviceprovider (ZSP) is een marktpartij die een beveiligde verbinding aanbiedt tussen een GBZ van een zorgaanbieder en het landelijk schakelpunt. Deze paragraaf beschrijft de beveiliging van deze dienst. De eisen die hiervoor gelden zijn opgenomen in het Programma van Eisen ZSP (PvE ZSP) . Zie ook de bijlage Normering informatiebeveiliging Landelijk EPD.

Beveiligingsbeleid

Een ZSP dient een beveiligingsplan op te stellen waarin is aangegeven welke maatregelen de ZSP heeft ingericht voor de beveiliging van alle netwerkkoppelingen (waaronder: met de beheersystemen, het landelijk schakelpunt, de GBZ'en, de SBV-Z en het UZI-register). De beheerder van de ZSP is verantwoordelijk voor de implementatie en handhaving van deze maatregelen en procedures.

Organisatieplan

In het organisatieplan dienen organisatorische taken, bevoegdheden en verantwoordelijkheden in het kader van informatiebeveiliging te worden toegekend aan de organisatie en de medewerkers van de ZSP. Het organisatieplan dient onder meer informatie over de organisatiestructuur, het personeelsbeleid, de huisvesting en een opleidingsplan te bevatten.

Eisen ten aanzien van personeel

Een ZSP dient zijn personeel geheimhoudingsverklaringen te laten ondertekenen. De geheimhouding heeft betrekking op persoonsgegevens en andere medische informatie. Bij beëindiging van de relatie met de werknemer of externe partij dient een procedure te worden gevolgd voor het intrekken van toegangsrechten.

Fysieke beveiliging

De apparatuur van de ZSP bevindt zich in een fysiek beveiligde omgeving en is slechts toegankelijk voor geautoriseerd personeel van de ZSP. Apparatuur van de ZSP is zodanig

geplaatst en beveiligd dat de risico's van schade en storing van buitenaf en de kansen op ongeautoriseerde toegang minimaal is.

Bescherming aangesloten partijen

De ZSP vrijwaart het landelijk schakelpunt en aangesloten GBZ'en van spam, virussen en overige dreigingen van andere systemen die – via het openbare internet of anderszins – toegang hebben tot het netwerk van de ZSP.

Naleving en beveiligingsincidenten

Ten behoeve van de controle op de juiste werking en de navolging van de juiste procedures worden alle beheerhandelingen vastgelegd in een logboek. Periodiek, of wanneer daar aanleiding toe is, kan een audit op de ZSP worden uitgevoerd.

Goed beheerd zorgsysteem (GBZ)

De opslag van patiëntgegevens in het kader van de gegevensuitwisseling via de landelijke infrastructuur vindt gedecentraliseerd plaats in het 'bronsysteem' van de verantwoordelijke zorgaanbieder (zie ook de bijlage). De zorgaanbieder blijft zelf verantwoordelijk voor de correctheid en de vertrouwelijkheid van deze gegevens.

Om te kunnen aansluiten op AORTA dient een bronsysteem te zijn gekwalificeerd als een goed beheerd zorgsysteem (GBZ). De eisen waaraan een GBZ moet voldoen, zijn beschreven in het Programma van Eisen GBZ (PvE GBZ). Deze paragraaf beschrijft de maatregelen die zijn genomen om de kwaliteit en beveiliging van een GBZ te waarborgen. Zie ook de bijlage Normering informatiebeveiliging Landelijk EPD.

Beveiliging

De patiëntgegevens in het GBZ dienen beveiligd te zijn tegen ongeautoriseerde toegang.

Alleen zorgaanbieders en door hen gemandateerde medewerkers kunnen via het GBZ met behulp van de persoonlijke UZI-pas patiëntgegevens opvragen.

Op grond van de NEN 7510 zijn zorgaanbieders verplicht een risicoanalyse uit te voeren met betrekking tot hun informatiesystemen en alle externe verbindingen en dienen zij aanvullende beveiligingsmaatregelen maatregelen te nemen voor de risico's die hierin worden onderkend.

Het GBZ zelf moet voorzien zijn van een UZI-certificaat om patiëntgegevens te kunnen uitwisselen via een beveiligde verbinding met het landelijk schakelpunt.

Beschikbaarheid

Zorgaanbieders dienen vierentwintig uur per dag patiëntgegevens te kunnen leveren. Dit stelt hoge eisen aan de beschikbaarheid van een GBZ. Voor de zorgaanbieder betekent dit dat hij zijn GBZ professioneel moet (laten) beheren. Dit vergt periodieke controle en eventueel preventief onderhoud. Verder moet een onverhoopte storing meteen worden gesignaleerd, zodat een GBZ-beheerder snel beschikbaar kan zijn om het probleem te verhelpen.

Logging

Het GBZ dient een logging in stand te houden waarin alle ontvangen opvraagberichten en verzonden opleverberichten tussen zorgaanbieders worden vastgelegd evenals de gebruikershandelingen op het GBZ.

2. Security monitoring

Op het bestaande landelijk schakelpunt zijn door Nictiz processen ingericht om controle en toezicht op rechtmatige toegang tot gegevens vast te stellen. Deze processen zullen vooralsnog worden voortgezet in de doorstartsituatie. Er wordt hier verwezen naar het vertrouwelijke document over Security Monitoring, dat als bijlage bij het doorstartmodel is toegestuurd in het kader van het zienswijzeverzoek aan het CBP. Met de Verantwoordelijke (VVZ) zullen afspraken en procedures met betrekking tot toezicht op gebruik en vermeend misbruik nader worden uitgewerkt.

3. Toelichting op toetsing behandelrelatie

In het voorgelegde doorstartmodel is aangegeven dat in het autorisatieproces mede wordt getoetst of sprake is van een behandelrelatie. Dit document geeft hierop een toelichting.

Hieronder is kort toegelicht hoe het autorisatieproces verloopt, hoe de toetsing van de behandelrelatie in zijn werk gaat en welke aanvullende maatregelen in de toekomst kunnen worden getroffen.

Het autorisatieproces
De autorisatie van zorgaanbieders met betrekking tot index- en patiëntgegevens verloopt in twee stappen:

1. in het goed beheerd zorgsysteem (GBZ) wordt getoetst of de zorgaanbieder een behandelrelatie heeft met de patiënt van wie hij gegevens wenst op te vragen;
2. de opvraging wordt getoetst aan het autorisatieprotocol. Hierin is, aan de hand van BIG-rolcodes, vastgelegd welke bevoegdheden de zorgaanbieder op grond van zijn zorginhoudelijke rol en functie heeft.

Toetsing behandelrelatie
De toegang tot de landelijke infrastructuur is uitsluitend voorbehouden aan zorgaanbieders die een behandelrelatie hebben met de betreffende patiënt. Voorafgaand aan het verlenen van toegang tot de verwijsindex en patiëntgegevens wordt de behandelrelatie getoetst. Deze toetsing vindt decentraal plaats op het niveau van het GBZ. De eisen die ten aanzien van het toetsen van de behandelrelatie aan de GBZ applicatie worden gesteld zijn vastgelegd in het Programma van Eisen (PvE) GBZ. Deze eisen worden tijdens een kwalificatie getoetst.

De toetsing van de behandelrelatie verloopt in de hieronder genoemde stappen. De stappen a t/m c betreffen een technische toetsing. Een schematische weergave is opgenomen als bijlage.

A: Is de patiënt ingeschreven in het opvragend goed beheerd zorgsysteem (GBZ)?
Allereerst wordt nagegaan of de patiënt is ingeschreven in de patiëntenadministratie van de zorgaanbieder die patiëntgegevens wenst op te vragen. Voor dit doel wordt nagegaan of het burgerservicenummer van de patiënt voorkomt in deze administratie en of dit geverifieerd is.

Indien de patiënt niet is geregistreerd in het GBZ wordt de toegang tot de landelijke infrastructuur geweigerd.

B1: Heeft de beroepsbeoefenaar eerder patiëntgegevens van deze patiënt aangemeld bij het landelijk schakelpunt?

Indien de beroepsbeoefenaar eerder patiëntgegevens van de patiënt heeft aangemeld, wordt hieruit op GBZ-niveau afgeleid dat er een behandelrelatie met deze patiënt bestaat. Vervolgens wordt nagegaan of de behandelrelatie nog steeds aanwezig is (zie B2). Indien geen sprake is van een eerdere aanmelding, wordt nagegaan of de behandelrelatie blijkt uit de werkcontext (zie onder C).

B2: Is de behandelrelatie nog steeds aanwezig?
Om er zeker van te zijn dat de behandelrelatie nog steeds bestaat, wordt geverifieerd of de behandelrelatie niet inmiddels is verlopen of expliciet is beëindigd. Als dit niet het geval is, wordt de aanvraag doorgeleid naar het autorisatieprotocol. Hierin is voor ieder type beroepsbeoefenaar vastgelegd tot welke gegevens hij toegang krijgt en welke gebruikshandelingen hij mag verrichten. Indien de behandelrelatie inmiddels beëindigd is, wordt nagegaan of er sprake is van een nieuwe behandelrelatie die blijkt uit de werkcontext (zie onder C).

C: Blijkt de behandelrelatie met de beroepsbeoefenaar uit de werkcontext?
Indien de opvragende beroepsbeoefenaar niet eerder patiëntgegevens van de patiënt heeft aangemeld bij het landelijk schakelpunt (zie B1) kan de behandelrelatie in bepaalde gevallen worden afgeleid uit de context waarin de aanvraag wordt gedaan. Dit is het geval wanneer:

- in het GBZ, bijvoorbeeld in een ziekenhuis, is geregistreerd dat de betreffende patiënt een afspraak heeft met een specifieke arts of specialist;

- de apotheker een recept heeft ontvangen van de huisarts;

- een verwijzing naar de zorgaanbieder is geregistreerd;

- de patiënt in het kader van een verzoek van de zorgaanbieder tot het verrichten van onderzoek is geregistreerd in het systeem van een laborant.

- de zorgaanbieder een dossier voert over de betreffende patiënt.

D: De beroepsbeoefenaar dient de behandelrelatie en de toestemming van de patiënt expliciet te bevestigen.
Indien de behandelrelatie niet blijkt uit de werkcontext dan wel de stappen onder B, dient de beroepsbeoefenaar de behandelrelatie expliciet te bevestigen. Deze bevestiging geschiedt via een bevestigingsscherm. Indien deze bevestiging wordt gegeven, wordt de opvraging doorgeleid naar het autorisatieprotocol. Indien deze bevestiging uitblijft, wordt de toegang geweigerd.