Ministerie van Volksgezondheid,
Welzijn en Sport

> Retouradres Postbus 20350 2500 EJ Den Haag

De heer G. van 't Noordende
System and Network Engineering (SNE) groep
Faculteit der Natuurwetenschappen, Wiskunde en Informatica (FNWI)
Universiteit van Amsterdam
Science Park 107
1098 XG AMSTERDAM

Macro Economische Vraagstukken en Arbeidsvoorwaardenbeleid

Bezoekadres:
Parnassusplein 5
2511 VX Den Haag
T 070 340 79 11
F 070 340 78 34
www.minvws.nl

Inlichtingen bij

T 070 340

Ons kenmerk
MEVA/ICT-2996404

Bijlagen
4

Uw brief

Correspondentie uitsluitend richten aan het retouradres met vermelding van de datum en het kenmerk van deze brief.

Datum 30 MRT 2010
Betreft Uw brief inzake de beveiliging van het Landelijk EPD

Geachte heer Van 't Noordende,

Met interesse heb ik kennisgenomen van uw brief aangaande de informatiebeveiliging van het landelijk EPD van 25 februari jl., de bijgevoegde samenvatting van constateringen en aanbevelingen en uw artikel 'A Security Analysis of the Dutch Electronic Patient Record System'.

Hieronder zal ik ingaan op de door u gedane constateringen ten aanzien van de architectuur en protocollen zoals die zijn beschreven in de AORTA-architectuurdocumentatie. Ik hecht er waarde aan om daarbij een aantal aspecten ten aanzien van de *operationele invoering* van het landelijk Elektronisch Patiëntendossier (EPD) toe te lichten aangezien deze geen onderdeel hebben uitgemaakt van uw onderzoek.

Alvorens in te gaan op de door u gedane constateringen wil ik u er op wijzen dat de AORTA-architectuur tot stand is gekomen met optimale informatiebeveiliging als uitgangspunt. Hierbij is rekening gehouden met de praktijksituaties in de gezondheidszorg. Dit betekent dat gekozen oplossingen kunnen verschillen van het theoretische maximum aan informatiebeveiliging. Waar noodzakelijk zijn resulterende risico's met aanvullende procedurele en technische maatregelen afgedekt. De praktijkimplementatie is en wordt periodiek getest (zie bijlage 1 - Grootschalige Ketenbrede Indringerstesten) en getoetst (zie bijlage 2 - Toetsingen van praktijkimplementaties).

Alle door u beschreven risico's zijn onderwerp van nadrukkelijke en zorgvuldige afweging in de ontwerpfase geweest. Dat een andere keuze is gemaakt dan waar uw voorkeur naar zou uitgaan, komt veelal vanwege een andere beoordeling van de kans op en de gevolgen van de risicosituatie gegeven de getroffen aanvullende maatregelen.

1 Noodzaak end-to-end authenticatie

In uw brief geeft u aan dat de op het LSP aangesloten GBZ systemen op dit moment geen mogelijkheid hebben om onafhankelijk van het LSP te verifiëren of een inkomend verzoek om patiëntgegevens op te vragen daadwerkelijk afkomstig is van een zorgverlener en dat op dit moment de noodzakelijke end-to-end authenticatie ontbreekt.

Voor het LSP gelden strenge beveiligingseisen voor ontwikkeling, implementatie en beheer die jaarlijks door onafhankelijke derden worden getoetst door middel van audits en indringerstesten. 'End-to-end' berichtenauthenticatie zoals door u voorgesteld kan bijdragen aan de veiligheid wanneer het LSP door een GBZ niet meer als een te vertrouwen connectiepunt gezien kan worden (bijvoorbeeld omdat een indringer in staat is malafide software in het LSP te installeren). Een dergelijk risico is echter ondervangen met een groot aantal technische en procedurele maatregelen.
Op basis van de in bijlage 1 en 2 beschreven testen en toetsingen is er tot op heden geen aanleiding geweest om voor implementatie van end-to-end authenticatie te kiezen. Daarnaast zou de doorvoering van uw aanbevelingen leiden tot een significante toename van de complexiteit van de implementatie GBZen met mogelijke nieuwe implementatie-, beheer- en beveiligingsrisico's als gevolg.

2 Huidige wijze van mandatering

Ten aanzien van uw kritiek op het mandateringsmodel het volgende.
Mandatering is noodzakelijk om de zogenaamde 'verlengde arm constructie' adequaat te kunnen ondersteunen. Deze constructie (zie artikel 38 Wet BIG) komt vaak voor in de medische praktijk en houdt in dat BIG-geregistreerden (aan wie bepaalde handelingen voorbehouden zijn) aan niet-BIG geregistreerden (bijvoorbeeld doktersassistenten) opdracht kunnen geven om onder diens verlengde verantwoordelijkheid handelingen te verrichten. Uitgangspunt in de wetgeving is dat het de beroepsbeoefenaar is die toegang heeft tot het landelijk EPD, onder beroepsbeoefenaar vallen BIG-geregistreerden.
Het door u aangedragen risico met betrekking tot mandatering vergt een situatie waarin een indringer met de benodigde technische systeem-, programmeer- en HL7-kennis de mogelijkheid heeft om de systeemfunctionaliteit zodanig te manipuleren dat de mandateringstabel wordt omzeild. Daarnaast dient de indringer voor het insturen van berichten de beschikking te hebben over een geldige UZI-pas (die niet is ingetrokken door de eigenaar) met de juiste autorisaties voor het uitvragen van de gewenste gegevens en de bijbehorende PIN-code.
In het licht van een zorgvuldige afweging tussen het potentiële risico van misbruik van mandatering en werkbaarheid van procedures in de praktijk, is gekozen voor decentrale registratie van mandateringsrelaties. Hierbij is uitgegaan van een goede balans tussen een adequaat beveiligingsniveau en een werkbare praktijksituatie. Een methodiek van centrale registratie vergt daarentegen nieuwe registratieprocessen binnen zorginstellingen voor het aanmelden, wijzigen en afmelden van mandateringsrelaties bij het LSP.
Daarnaast worden dergelijke risico's gemonitord via praktijktoetsingen (zie bijlage 2 - Toetsingen van praktijkimplementaties) en de hiervoor reeds genoemde indringerstesten in de GKI (zie bijlage 1 -Grootschalige Ketenbrede Indringerstesten).

Een ander door u aangevoerd punt van kritiek ten aanzien van het mandateringsmodel betreft het feit dat medewerkers op dit moment de volledige rechten van de mandaterende zorgverlener krijgen. U pleit er dan ook voor om interacties die een nieuwe behandelrelatie impliceren, maar ook de registratie van (nieuwe) gegevens in het LSP voor te behouden aan zorgverleners.
Dit acht u van belang onder meer gezien de (volgens u) slechte controleerbaarheid van mandateringen en aansprakelijkheidskwesties.

Binnen het huidige mandateringsmodel zijn alle mandateringen echter te controleren. Allereerst worden UZI-passen via een UZI-abonnee verstrekt en worden deze ofwel op naam verstrekt van de betreffende zorgverlener (een BIG-geregistreerde) of op naam van een medewerker van de UZI-abonnee. UZI-passen kunnen ook niet op naam maar op functie worden uitgegeven onder vermelding van de naam van de UZI-abonnee. In het laatste geval is de UZI-abonnee op wiens naam deze passen worden verstrekt direct verantwoordelijk voor de medewerkers die van deze passen gebruik maken. Met de UZI-pas niet op naam is toegang tot het EPD niet mogelijk. Met medewerkers aan wie UZI-passen op naam worden verstrekt dient de UZI-abonnee (schriftelijke) afspraken te maken over het gebruik van de pas. Daarnaast wordt het *gebruik* van mandateringen centraal gelogd en geanalyseerd. De mandaterende zorgverlener is verantwoordelijk voor het inrichten en het inzichtelijk maken voor inspectie van de mandateringstabel. Daarmee is deze zorgverlener tevens aansprakelijk voor de handelingen van zijn medewerkers via gemandateerde berichten. Bij de GBZ-schouwingen die periodiek worden uitgevoerd door Nictiz (zie bijlage 2 - Toetsingen van praktijkimplementaties) wordt expliciet vastgesteld dat de procedure mandaatbeheer is vastgelegd. In de procedure dient in ieder geval het beheer van bevoegdheden op het GBZ en het beheer van de UZI-pas te zijn vastgelegd. Tijdens de XIS-kwalificaties wordt expliciet getoetst of de GBZ applicatie voldoet aan de eisen om mandatering correct uit te kunnen voeren.

3 Opslag van loggegevens in het LSP

Ten behoeve van het toezicht op het gebruik van het landelijk EPD door de IGZ en het CBP wordt het gebruik gelogd. Om het toezicht zo effectief en efficiënt mogelijk te laten verlopen worden loggegevens op basis van gedefinieerde use cases automatisch geanalyseerd en kunnen onregelmatigheden worden gedetecteerd. De loggegevens worden alleen bewaard om na het signaleren van onregelmatigheden te kunnen reconstrueren welke gegevens zijn aangemeld of opgevraagd. Uw constatering dat op verzoek van een zorgconsument verwijsgegevens in het LSP wel worden verwijderd, maar (historische) loggegevens niet, geldt alleen voor zorgconsumenten waarvan indexgegevens aanwezig waren in het LSP die later via een totaalbezwaar zijn verwijderd. Hierbij heeft een afweging plaatsgevonden tussen de verwijdering van loggegevens via totaal bezwaar enerzijds en de noodzaak van (historische) loggegevens voor het kunnen reconstrueren van onrechtmatig gebruik (aanmelding/opslag) anderzijds. Wanneer hiertoe aanleiding bestaat zal deze afweging opnieuw plaatsvinden.

4 Tekortkoming DigiD met SMS authenticatie

Ten aanzien van uw suggesties voor berichtautorisatie door zorgconsumenten op basis van een PKI-authenticatiemiddel, zoals de elektronische Nationale Identiteitskaart (eNIK), verwijs ik u naar de bijgevoegde brief zoals deze op 12 december 2008 naar de Tweede Kamer is verzonden (Bijlage 3 – MEVA/ICT-2899251). Omdat de eNIK niet binnen de realisatietermijnen voor het landelijk EPD beschikbaar komt, is gekozen voor EPD-DigiD (gebruikmakend van DigiD op basis van SMS-authenticatie en een face-to-face uitgifteproces) als authenticatie-middel voor zorgconsumenten.

De realisatie daarvan wordt gebaseerd op het adviesrapport[1] waarnaar u in uw brief en artikel refereert.

5 Informed consent

U geeft aan een aantal verbeterpunten te zien ten aanzien van het huidige informed consent model. Zo pleit u er voor om zorgconsumenten de mogelijkheid te bieden om aan te geven dat hen eerst om toestemming moet worden gevraagd alvorens (nieuwe) gegevens in het EPD mogen worden aangemeld.
Er is voor het huidige informed consent model gekozen om te borgen dat binnen een afzienbare tijd medische gegevens van een groot deel van de zorgconsumenten in Nederland kunnen worden uitgewisseld tussen zorgverleners. Dit is noodzakelijk om de doelstellingen en daarmee de boogde toegevoegde waarde van het landelijk EPD te kunnen realiseren. Om te zorgen dat de informatie wel beschikbaar kan worden gesteld, geldt een systeem van opt-out voor het aanmelden van de gegevens waarbij gegevens worden aangemeld tenzij zorgconsumenten bezwaar hebben gemaakt tegen de uitwisseling van gegevens via het landelijk EPD. De indexgegevens van zorgconsumenten die bezwaar hebben gemaakt worden dan uit de verwijsindex binnen het LSP verwijderd. Voordat een zorgaanbieder gegevens kan raadplegen is toestemming van de patiënt nodig (opt-in). Op deze wijze wordt toestemming gevraagd voordat gegevens worden geraadpleegd. De mogelijkheid om bezwaar te kunnen maken is een extra faciliteit die wordt geboden om de zorgconsument de mogelijkheid te geven geen gegevens beschikbaar te stellen via het landelijk EPD.
Eind 2008 zijn zorgconsumenten via een voorlichtingscampagne op de hoogte gebracht van de wijze waarop gegevensuitwisseling via het landelijk EPD plaatsvindt en hoe het gehanteerde informed consent model werkt. Daarnaast krijgt iedere zorgconsument een notificatiebrief wanneer de eerste indexgegevens in het LSP worden aangemeld door een zorgverlener. Daarbij wordt tevens op de mogelijkheid van het maken van bezwaar gewezen.
Zorgconsumenten hebben nu al de mogelijkheid om via een aanvraagformulier inzage te vragen in welke gegevens worden uitgewisseld via het landelijk EPD en welke zorgverleners deze gegevens hebben opgevraagd.

Met het Klantenloket en Toegang Patiënt krijgen zorgconsumenten via het internet de mogelijkheid om loggegevens in te zien, de eigen medische gegevens te raadplegen en bezwaar voor de uitwisseling van medische gegevens via het landelijk EPD in te dienen. Hiermee nemen de mogelijkheden voor inzage en controle door zorgconsumenten ten aanzien van de eigen medische gegevens toe ten opzichte van de huidige elektronische en papieren medische dossiers.

[1] Beveiligingeisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Elektronisch Patiëntendossier (EPD), PricewaterhouseCoopers Advisory, het Institute for Computing and Information Sciences van de Radboud Universiteit Nijmegen en het Tilburg Institute for Law, Technology and Society van de Universiteit van Tilburg, 2 december 2008.

Macro Economische Vraagstukken en Arbeidsvoorwaardenbeleid

Ons kenmerk
MEVA/ICT-2996404

Tot slot wil ik u erop wijzen dat aan de hand van een managementcyclus (zie bijlage 2 - Toetsingen van praktijkimplementaties), bedreigingen ten aanzien van de informatiebeveiliging voor het landelijk EPD op een continu basis worden geïnventariseerd, geanalyseerd en geadresseerd.

Hoogachtend,

de Minister van Volksgezondheid,
Welzijn en Sport,
namens deze,
de Directeur-Generaal Landurige Zorg,

drs. M.J. Boereboom

Bijlagen:

Bijlage 1 - Grootschalige Ketenbrede Indringerstesten

Bijlage 2 - Toetsingen van praktijkimplementaties

Bijlage 3 – MEVA/ICT-2899251

Bijlage 4 – MEVA/ICT-2984098

Kopie verzonden aan: Gert-Jan van Boven, directeur Nictiz

Bijlage 1 - Grootschalige Ketenbrede Indringerstesten

Macro Economische Vraagstukken en Arbeidsvoorwaardenbeleid

Ons kenmerk
MEVA/ICT-2996404

Bij de wetsbehandeling 'Wijziging van de Wet gebruik Burgerservicenummer in de zorg in verband met de elektronische informatieuitwisseling in de zorg' (EPD-wet) in de Tweede Kamer is aangegeven dat voorafgaand aan het verplicht aansluiten van GBZen op het LSP, het landelijk EPD aan een Grootschalige Ketenbrede Indringerstest (GKI) zal worden onderwerpen. Het doel van de GKI is de veilige en betrouwbare gegevensuitwisseling binnen de AORTA-infrastructuur aan te tonen.

De GKI bestaat uit de volgende set van indringerstesten:
1 Indringerstest SBV-Z.
2 Indringerstest UZI-Register.
3 Indringerstest LSP.
4 Representatieve steekproeven GBZ.
5 EPD-keten Indringerstesten op de Schakelconnecties (EIS).

Voor het Klantenloket en Toegang Patiënt worden indringerstesten meegenomen in de ontwikkeling die gereed zijn bij het beschikbaar komen van deze faciliteiten. Eventuele bevindingen voortkomend uit de genoemde indringerstesten worden geanalyseerd waarna op basis van een risico-inschatting eventuele additionele procedurele en/of technische maatregelen worden geïmplementeerd. .
Voor de meest recente status van de GKI verwijs ik u naar de bijgevoegde voortgangsrapportage zoals deze op 8 februari 2010 naar de Tweede Kamer is verzonden (Bijlage 4 – MEVA/ICT-2984098).

Gezien de directe relevantie met uw onderzoek licht ik kort de uitvoering van EIS als onderdeel van de GKI toe. EIS betreft een technische test waarbij negatief getoetst wordt of de connecties en connectiepunten tussen GBZen en ZSPs voldoen aan de eisen zoals deze zijn beschreven in het PvE GBZ en het PvE ZSP.

Hierbij zal gekeken worden naar:
- Netwerkbeveiliging van de IP-adressen en netwerkpoorten.
- Applicatieve beveiliging voor achter netwerkpoorten luisterende (web)services.
- Berichtenbeveiliging voor uitvragen, ontvangen, lezen en verwerken van HL7-berichten.

Een aantal door u geschetste risico's ten aanzien van aanvallen van netwerken en informatiesystemen en de manipulatie van berichten door hackers worden meegenomen bij de uitvoering van EIS.

Bijlage 2 - Toetsingen van praktijkimplementaties

Een zorginstelling die voornemens is aan te sluiten op het landelijk EPD dient in eerste instantie te beschikken over een implementatie van een gekwalificeerde XIS-applicatie. Door middel van een XIS-typekwalificatie wordt door Nictiz getoetst of een softwareproduct van een leverancier voldoet aan de applicatie-eisen zoals deze zijn beschreven in het Programma van Eisen voor een Goed Beheerd Zorgsysteem (PvE GBZ).

De implementatie en het beheer van het XIS-applicatie wordt geborgd via de implementatie- en exploitatie-eisen beschreven in het PvE GBZ. Controle op de naleving van deze eisen door zorgverleners geschied op basis van GBZ-schouwingen die periodiek worden uitgevoerd in opdracht van Nictiz.

Een GBZ moet gebruik maken van een gekwalificeerde Zorg Service Provider (ZSP), die de netwerkdiensten levert, voor de aansluiting op het Landelijk Schakelpunt (LSP). In opdracht van Nictiz worden ZSPs gekwalificeerd aan de hand het Programma van Eisen voor een Zorg Service Provider (PvE ZSP).

Een zorginstelling kan alleen aansluiten op het landelijk EPD met een gekwalificeerde XIS-applicatie, een gekwalificeerde ZSP en een ondertekende eigenverklaring over de naleving van de geldende beveiligingseisen. Daarnaast dienen zorginstellingen via het besluit onderliggend aan de huidige Wet op het gebruik van het Burgerservicenummer in de zorg te voldoen aan de NEN 7510 norm voor informatiebeveiliging in de zorg. Toezicht hierop vindt plaats door de toezichthouders Inspectie van de Gezondheidszorg (IGZ) en het College Bescherming Persoonsgegevens (CBP). Een voorbeeld hiervan is het in oktober 2008 door IGZ en CBP gepubliceerde onderzoek over de status van informatiebeveiliging in 20 Nederlandse ziekenhuizen.

De bij het landelijk EPD betrokken beheerorganisaties borgen een adequaat informatiebeveiligingsniveau met een managementcyclus bestaande uit het:

- Plannen van informatiebeveiligingsmaatregelen (uitvoeren periodieke risicoanalyses en opstellen en onderhouden van een informatiebeveiligingsbeleid).
- Implementeren van informatiebeveiligingsmaatregelen (op basis van het informatiebeveiligingsbeleid en standaarden zoals VIR, NEN 7510, ISO 27001/27002 en ITIL).
- Controleren van een correcte implementatie van de voorgenomen maatregelen (door middel van eenmalige en periodieke interne en externe audits en toetsingen).
- Bijsturen op basis van de bevindingen uit de periodieke audits en toetsingen.