



Interpay

Adviesrapport ICT-beveiliging in de Zorg
Ministerie van VWS

Interpay

16 oktober 2006

Adviesrapport ICT-Beveiliging in de Zorg


Ministerie van VWS

Interpay

Datum	16 oktober 2006
Auteur(s)	R.A. van Erk, J.G. van Dongen
Project Manager	Drs. H.J.W.M. Luijks

All rights reserved.

No part of this publication may be reproduced and/or published by print, photo print, microfilm or any other means without the previous written consent of Interpay Nederland B.V.

A decorative blue line that starts as a horizontal line on the left and curves upwards on the right side.

Inhoud

1	Introductie.....	6
2	Doel, reikwijdte en resultaten adviesrapport.....	7
2.1	Doel.....	7
2.2	Reikwijdte	7
2.3	Resultaten	7
3	Management summary	9
3.1	Algemeen beeld	9
3.1.1	EPD beleving	9
3.2	Cultuur.....	10
3.3	Conclusies en adviezen	10
3.3.1	Normering	10
3.3.2	Eisen.....	10
3.3.3	Certificering	11
3.3.4	Organisatorische aspecten	11
3.3.5	Regio versus landelijk.....	11
3.3.6	Privacy versus betrouwbaarheid	12
3.3.7	Loketfunctie	12
3.3.8	Invoering informatiebeveiliging.....	13
3.3.9	Beveiligingsbewustzijn.....	13
4	Beleid, Naleving en Sancties.....	14
4.1	Toezichthouder	14
4.1.1	Toezichthoudende rol	14
4.1.2	Doelstelling.....	14
4.1.3	Kaders en reikwijdte	14
4.1.4	Instrumenten	15
4.1.5	Rollen van belanghebbende.....	16
4.1.6	Toezichthoudende rol zoals deze is waargenomen in de zorgsector	16
4.2	Interbancair overlegorgaan geënt op informatiebeveiliging	16
4.3	Sancties	17
5	Escalatie en Communicatie.....	18
5.1	Continuïteit van de bedrijfsvoering	18
5.1.1	Crisis management Team en Escalatie	18
5.2	Integriteit van het betalingsverkeer	18
5.2.1	Inleiding	18
5.2.2	Aanbevelingen voor de zorgsector.....	18
6	Certificeren en Toezicht	20
6.1.1	Inleiding	20
6.1.2	Proces van certificeren van betaalautomaten t.b.v. het merk 'PIN'	20
6.1.3	Proces van certificeren van systemen die aansluiten op het LSP.....	21
6.1.4	Aansluitvoorwaarden versus gebruikerswensen	22
6.1.5	Implementatie-eisen	22
6.1.6	Bestaande wetten (WBP, WGBO, WGBZ), regels en normen (NEN7510) ...	23
6.2	Aanbevelingen voor de zorgsector	23
7	Keymanagement, Organisatie en apparatuur	26
7.1	Keymanagement en kaartgebruik	26
7.1.1	KMC en Interpay sleutelbeheer.....	26
7.1.2	Doelstelling.....	26
7.1.3	Beschrijving van de waargenomen situatie bij het UZI-register.....	26
7.2	Functionele inrichting.....	27
7.2.1	Functionele inrichting van plastic en bankkaarten	27
7.2.2	Doelstelling.....	28
7.2.3	Beschrijving huidige situatie smartcardgebruikt door het UZI register.....	28
7.2.4	Aanbevelingen voor de zorgsector.....	28
8	Preventie, detectie en repressie.....	29
8.1	Fraudepreventie en -repressie.....	29
8.1.1	Fraudebestrijding (repressief en preventief)	29

8.2	Fraudepreventie en -detectie	29
8.2.1	Doelstelling, waarom is het opgezet	29
8.2.2	Preventie, detectie en repressie binnen de zorg	30
8.2.3	Concrete aanbevelingen binnen de zorgsector:	30
9	Bijlagen	31
9.1	Gebruikte begrippen	31
9.2	Gebruikte afkortingen	32
9.3	Geraadpleegde literatuur	34
9.4	Geconsulteerde en geïnterviewde personen	34

1 Introductie

Onder regie van het ministerie van Volksgezondheid, Welzijn en Sport (VWS) is begin 2006 het Landelijk Schakelpunt voor de zorgsector opgericht. Het schakelpunt regelt onder meer de veilige, actuele elektronische uitwisseling van patiënteninformatie tussen alle partijen in de zorg.

Een geruisloos functionerend Landelijk Schakelpunt is een noodzakelijke voorwaarde voor de landelijke invoering van het Elektronisch Medicatie Dossier (EMD) en het elektronische Waarneem Dossier Huisartsen (WDH), de eerste hoofdstukken van een landelijk Elektronisch Patiënten Dossier (EPD).

De minister van VWS heeft besloten om in 2005 de eerste stappen te zetten voor de realisatie van het landelijke Elektronische Patiënten Dossier. In samenwerking met het agentschap Centraal Informatiepunt Beroepen Gezondheidszorg (CIBG), het Nationaal ICT Instituut in de Zorg (NICTIZ) en de betrokken branche- en koepelorganisaties in de zorgsector is het ministerie gestart met de invulling van het EPD.

Het belang van beveiligingsbewustzijn en beveiligingsniveau op bestuurlijk en technisch niveau vormt voor het ministerie aanleiding om in gesprek te komen met partijen die over de expertise beschikken om hen hierin te adviseren. In dit kader vond op 9 februari 2006 een gesprek plaats tussen de heer M. van Rijn (Directeur-Generaal Gezondheidszorg), mevrouw E. Maat (Hoofd Programma ICT in de zorg), de heer A. Kuijpers (Directeur Interpay) en de heer W. Machielse (Directieadviseur Interpay). Het hoge beveiligingsniveau van het Nederlandse betalingsverkeer, de in bijna veertig jaar opgebouwde ervaring in het betalingsverkeer en de expertise op het gebied van risk en security management van Interpay Nederland liggen hieraan ten grondslag. Centraal in dit gesprek stond de vraag in hoeverre Interpay het ministerie van VWS kan adviseren en of een vorm van samenwerking tussen beide partijen tot stand kan worden gebracht.

2 Doel, reikwijdte en resultaten adviesrapport

In de discussie over de beveiliging en privacy in de zorgsector wordt vaak verwezen naar het bankwezen en de wijze waarop daar het beveiligingsniveau en beveiligingsgedrag wordt gewaarborgd. Aan de Tweede Kamer is in november 2005 de toezegging gedaan om het bankwezen te benaderen. De aanwezige expertise wordt aangewend om de informatiebeveiliging in de zorgsector door te lichten en adviezen en/of aanbevelingen op te stellen waarmee een mogelijke achterstand van de beveiliging van de ICT in de zorgsector kan worden opgelost.

2.1 Doel

Op 15 februari 2006 heeft Interpay van mevrouw E.M. Maat de opdrachtomschrijving ontvangen.

De opdracht luidt als volgt: "het verkrijgen van gemeenschappelijk inzicht in de huidige mate van beveiliging van ICT in de zorgsector in relatie tot de invoering van het Elektronisch Patiënten Dossier (EPD) en maatregelen waarmee een mogelijke achterstand kan worden ingehaald, geborgd en gecontroleerd". Dit stelt het ministerie vervolgens in staat om het niveau van beveiliging van ICT in de zorgsector te bevorderen en de handhaving en bewaking te stimuleren.

De opdrachtomschrijving is op 19 juli aangescherpt. Het op te stellen adviesrapport dient voor een belangrijk deel te bestaan uit een beschrijving van de wijze waarop het bankwezen de beveiliging van het betalingsverkeer heeft ingericht en in hoeverre de beveiliging of maatregelen toepasbaar zijn in de zorgsector. Namens het ministerie waren mevrouw E.M. Maat en mevrouw E. Castelijn aanwezig, Interpay werd op 19 juli vertegenwoordigd door de heer H.J.W.M. Luijks, de heer R.A. van Erk en mevrouw K.T.J. Cardinaal – van de Laarschot.

2.2 Reikwijdte

Het ministerie van VWS heeft een zestal vragen voorgelegd aan Interpay:

- Kunt u een overzicht opstellen van relevante overeenkomstige ervaringen met de invoering van informatiebeveiliging vanuit Interpay?
- Kunt u een oordeel geven over het huidige beveiligingsniveau in de zorgsector?
- Kunt u een overzicht geven van de knelpunten van bestuurlijke, organisatorische, technische of juridische aard?
- Kunt u aanbevelingen doen om de mogelijke achterstand van beveiliging van ICT in de zorg op korte termijn in te halen?
- Kunt u aangeven welke wijzigingen noodzakelijk zijn op het gebied van organisatorische en bedrijfseconomische aard op het niveau van ziekenhuizen, huisartsenpraktijken en individuele zorgaanbieders?
- Kunt u aanbevelingen doen voor een moderne en efficiënte manier van toezicht op de naleving van beveiliging van ICT in de zorg?

Naar aanleiding van deze vragen heeft Interpay zich een beeld gevormd van het huidige beveiligingsniveau in de zorgsector. Zij heeft daartoe een beperkt aantal direct betrokkenen in de zorgsector geïnterviewd. Vervolgens beschrijft Interpay in dit adviesrapport de beveiligingsmaatregelen van het betalingsverkeer in de bancaire sector en een analyse van de bruikbaarheid ervan in de zorgsector.

2.3 Resultaten

Bij het hoofdstuk "Beleid, Naleving en Sancties" wordt ingegaan op welke wijze Interpay verplicht is om zich te houden aan bestaande regelgeving en op welke wijze hieraan een

invulling wordt gegeven.

Het hoofdstuk "Escalatie en Communicatie" gaat in op de werkwijze die Interpay hanteert bij grootschalige interbancaire problemen voor wat betreft de continuïteit van de bedrijfsvoering, de integriteit van het betalingsverkeer en de afstemming daarvan.

Het hoofdstuk "Certificeren en toezicht" geeft het model weer dat wordt gebruikt om te komen tot certificatie van betaalapparatuur. Daarnaast geeft dit hoofdstuk weer welke acceptatiecriteria kunnen worden gesteld, hoe hieraan door middel van deelcertificatie op een veilige en betrouwbare manier invulling wordt gegeven en op welke manier het toezicht wordt ingevuld.

Het hoofdstuk "Keymanagement, organisatie en apparatuur" beschrijft hoe Interpay omgaat met het sleutelbeheer van betalingsapparatuur en op welke wijze deze organisatorisch zijn ingebed.

Het hoofdstuk "Preventie, detectie en repressie" is gebaseerd op het naleven van regels en het voorkomen en bestrijden van fraude in de breedste zin van het woord.

3 Management summary

Interpay is als financieel dienstverlener binnen het Nederlandse betalingsverkeer gevraagd om ervaringen en mogelijke parallellen met de zorgsector op het gebied van informatiebeveiliging te delen met het ministerie van VWS. Dit heeft geresulteerd in een onderzoek dat van 1 juni 2006 tot 15 september 2006 is uitgevoerd. Gedurende dit onderzoek zijn gesprekken gevoerd met een representatieve afspiegeling vanuit de zorgsector, zoals vertegenwoordigers van zorginstellingen en zorgverleners en architecten welke oplossingen aandragen voor de invoering van een EPD binnen de zorgsector.

De methode die is gebruikt om tot de conclusies van dit rapport te komen is gebaseerd op interviews en desk research, gevoerd met de praktische ervaringen die Interpay heeft opgedaan met informatiebeveiliging.

Gelet op bovenstaande is het rapport dan ook geschreven vanuit het perspectief informatiebeveiliging. Onderwerpen die in dit rapport aan de orde komen zijn enerzijds geselecteerd op basis van enige overeenkomst met de zorgsector en anderzijds omdat zij stof tot nadenken geven die kunnen leiden tot implementatie ervan.

Het hoofdstuk "Certificeren en Toezicht" vormt naar de mening van Interpay de kern van het adviesrapport omdat hier de basiselementen en bouwstenen liggen voor een goed en gedegen landelijk werkend EPD. Indien aan deze basis afbreuk wordt gedaan kan dit ondanks andere technische toepassingen nooit leiden tot een EPD dat door het veld als veilig en betrouwbaar wordt beschouwd. Dit punt is cruciaal, vooral omdat patiënten exact willen weten hoe wordt omgesprongen met deze privacy gevoelige informatie en de elektronische opslag en uitwisseling ervan.

3.1 Algemeen beeld

Gedurende het onderzoek is gebleken dat bij de invoering van de hoofdstukken voor een landelijk EPD de beleving omtrent informatiebeveiliging zeer divers is. Bij de zorgverleners die enkelvoudig werken zoals de huisartsen is de verwachting dat zij te maken krijgen met ingrijpende wijzigingen om medische gegevens op een veilige manier te verwerken en uit te wisselen. De huidige eisen die worden gesteld zijn van dien aard dat deze groep er niet aan ontkomt aansluiting te zoeken bij een ASP, om te voldoen aan bijvoorbeeld de beschikbaarheidseis.

De apothekers, al dan niet geclusterd en ontsloten via overkoepelende instanties, staan voor wat betreft de invoering van het EMD voor de uitdaging om hun thans werkende (apotheek)applicaties gecertificeerd en opgenomen te krijgen in de landelijk beschikbare en toegankelijke applicaties via het LSP.

De groep van grote zorginstellingen (de ziekenhuizen) geven voor een deel de indruk nog onvoldoende budget ter beschikking te stellen om een en ander te kunnen regelen. De meest essentiële technische beveiligingsmaatregelen als virusscanners en firewalls zijn doorgaans aanwezig. Met name wordt thans nog onvoldoende aandacht besteed aan het belang van cultuur- en gedragsverandering en de noodzakelijke organisatorische maatregelen en procedurele aspecten om te kunnen voldoen aan de gewenste normen en standaards. Naast het stimuleren van investeren in informatiebeveiliging is ook een andere beveiligingsattitude noodzakelijk om een invoering van delen van het EPD succesvol te laten verlopen.

3.1.1 EPD beleving

De beleving van het onderwerp EPD is divers, dit wordt gevoerd door een eilandgevoel bij de

diverse belanghebbende partijen. Iedere partij interpreteert het begrip EPD verschillend. Voor de bedrijfsvoering wordt vooral gekeken naar de ontwikkelingen richting 3^e generaties EPD's die klinische paden ondersteunen. Dit in tegenstelling tot de huidige lokale EDP's die vooral als kijkdozen worden gezien. In de huidige situatie ontbreken duidelijke standaards voor de codering binnen de applicaties. Gegevens van de huidige lokale EPD's zijn veelal niet gestandaardiseerd en niet landelijk uitwisselbaar.

Een ander probleem voor zover het de medische gegevens betreft is de presentatie naar de patiënt die momenteel onbegrijpelijk is.

Een echt landelijk EPD wordt door de zorginstellingen niet binnen vijf jaar verwacht. Kenmerkend is de verwachting dat softwarefabrikanten gezien de beperkte Nederlandse markt niet in staat zullen zijn om volgende generaties EPD's te ontwikkelen.

Het toezicht op de invoering van een EPD, waarbij de diverse voorschriften en wettelijke kaders dienen te worden gevolgd, geeft voor de huidige toezichthouder in de gezondheidszorg een extra taak doordat nu ook specifiek gelet moet worden op ICT-onderwerpen. Dit is voor de Inspectie voor de Gezondheidszorg in haar rol als toezichthouder een zware taak aangezien zij daar thans niet voor is geëquipeerd.

3.2 Cultuur

Binnen de zorgsector wordt ICT veelal gezien als een ondersteunend proces. Binnen de bancaire wereld is ICT van begin af aan het uitgangspunt geweest en kan men spreken van primaire processen waarvan de bedrijfsvoering volledig afhankelijk is. De zorgsector dient op zorgvuldige wijze een cultuuromslag te maken waarbij ook wordt ingezien dat ICT een onderdeel is van het primaire proces voor de bedrijfsvoering.

Ondanks het feit dat de cultuurverschillen tussen de bancaire wereld en de zorgsector groot zijn, vallen er voldoende parallellen te onderkennen die een advies rechtvaardigen.

3.3 Conclusies en adviezen

In deze paragraaf zijn de belangrijkste aanbevelingen opgenomen. In het bijzonder binnen het hoofdstuk "Certificeren en Toezicht" worden ook andere aanbevelingen gedaan.

3.3.1 Normering

Het gebruik van instrumenten voor de informatiebeveiliging - specifiek de NEN-7510 norm, zijnde de voor de zorgsector toegespitste en afgeleide richtlijnen van de algemeen in gebruik zijnde Code van Informatiebeveiliging - is een kwaliteitsaspect die door het veld is gemaakt en geaccepteerd. Ondanks het draagvlak bij de theoretische totstandkoming van deze richtlijnen blijft de naleving in de praktijk achter. Hier dient een behoorlijke inhaalslag te worden gemaakt.

Interpay beveelt aan:

- a) het gebruik van de NEN-7510 monitor binnen de zorgsector meer te propageren. Met behulp van deze zelfanalyse zal binnen het veld een realistischer beeld worden gecreëerd van de (on)volkomenheden van de eigen organisatie;
- b) de normerende instantie NEN voor het veld controleerbare en toetsbare checklijsten te laten ontwikkelen die op dezelfde wijze gebruikt kunnen worden voor zorgverleners waar de NEN7510 monitor te grootschalig is voor gebruik.

3.3.2 Eisen

Vanuit het NICTIZ zijn de eisen aan te koppelen systemen en netwerken door middel van GBZ

en ZSP duidelijk geconcretiseerd. In dit kader moeten zij gezien worden als lokale eisen. Deze eisen zijn een verder uitgewerkte vertaling van de geaccepteerde NEN-normering, specifiek aangevuld om te kunnen werken met het Landelijk Schakel Punt. Specifieke eisen voor systemen en netwerken zijn noodzakelijk om eenduidigheid in onderlinge communicatie, transport van gegevens en de mate van beveiliging te bewerkstelligen. Indien deze acceptatiecriteria volledig worden nageleefd lijkt niets een verdere succesvolle implementatie van de diverse EPD hoofdstukken meer in de weg te staan. Onduidelijker is het beeld dat naar boven komt in het licht van landelijke eisen die gesteld moeten worden aan de volledige landelijke infrastructuur voor wat betreft dezelfde criteria.

Interpay beveelt aan:

c) een onafhankelijk partij een risicoanalyse te laten verrichten naar de kwetsbaarheden bij de implementatie van criteria, zoals die genomen zijn bij de werking van een landelijke infrastructuur voor het EPD.

3.3.3 Certificering

Het certificeren volgens de GBZ- en ZSP-eisen is een complex geheel omdat er een grote diversiteit aan GBZ systemen is met daarop draaiende zorgondersteunende applicaties. Ook zijn veel GBZ-systemen op de een of andere manier gekoppeld aan andere systemen. Hiermee is het volledig voldoen aan de GBZ eisen een langdurig en moeizaam proces.

Interpay beveelt aan:

d) een scheiding aan te brengen in het certificeringmodel waarbij een onderscheid wordt gemaakt tussen een beveiligingsdeel(verplicht) en een functioneel deel(deels verplicht).

3.3.4 Organisatorische aspecten

In het kader van de zware taak voor de Inspectie voor de Gezondheidszorg (mede gelet op de 'roep' voor een loketfunctie vanuit de patiënt en de noodzaak van een certificerende instantie) is het van belang om deze rollen te onderkennen en gescheiden in het leven te roepen, waarbij ieder orgaan verantwoording dient af te leggen aan het hoogste orgaan namelijk de Inspectie voor de Gezondheidszorg. Het is de ervaring van Interpay dat alleen door een duidelijke functiescheiding de kwaliteit van de zorgondersteunende systemen, het communicatiekanaal naar de patiënt en een onafhankelijke monitor binnen de zorgsector gewaarborgd kunnen worden.

Interpay beveelt aan:

e) het hoofdtoezicht op de invoering en naleving van de EPD voor wat betreft de ICT bij de Inspectie voor de Gezondheidszorg te leggen;

f) een onafhankelijke instantie te benoemen die rapporteert aan de Inspectie voor de Gezondheidszorg en als taakstelling krijgt om een loketfunctie op te zetten als spreekbuis voor publieke zaken omtrent het EPD;

g) beleg het toezicht en het certificeren van de diverse GBZ en ZSP systemen bij een onafhankelijke instantie, die rapporteert aan de Inspectie voor de Gezondheidszorg.

3.3.5 Regio versus landelijk

Wanneer legacy systemen al zijn opgenomen in regio's ontstaan hieruit diverse functioneel goed werkende processen. Hoewel deze systemen thans nog niet voldoen aan de gestelde GBZ-eisen lijkt het niet raadzaam om aan de al opgebouwde functionaliteit voorbij te gaan. Hoewel er beveiligingscommissies zitten in de regionale versus landelijke functionaliteit verdient