VP Huisartsen
vereniging praktijkhoudende huisartsen

Aan de voorzitter van de Normcommissie 303006
Informatievoorziening in de zorg
Mevrouw Marlou Bijlsma
Nederlands Normalisatie-instituut
Postbus 5059
2600 GB DELFT
communicatie@nen.nl

Amsterdam 31-01-2014

Commentaar op de conceptherziening van de NEN-norm 7512:2005

Geachte voorzitter,

De Vereniging Praktijkhoudende Huisartsen (VPHuisartsen) wil haar standpunt over de conceptherziening van de NEN-norm 7512:2005 langs deze weg overbrengen.

VPHuisartsen is een vereniging die maximaal invloed wil uitoefenen op de positionering in de gezondheidszorg van praktijkhoudende huisartsen en op de randvoorwaarden waaronder zij hun vak willen praktiseren. De vereniging telt circa 725 leden.

Bodemprocedure tegen VZVZ/LSP

De huisarts in Nederland heeft te maken met de moeizame introductie van een landelijk elektronisch communicatiesysteem: het Landelijk SchakelPunt(LSP).
Het is u wellicht bekend dat VPHuisartsen in 2013 een bodemprocedure heeft aangespannen tegen de Vereniging van Zorgaanbieders voor Zorgcommunicatie (VZVZ) die het LSP beheert.
Op de website van VPHuisartsen is een samenvatting van de dagvaarding te vinden.
http://www.vphuisartsen.nl/wordpress/wp-content/uploads/2013/03/Samenvatting_Dagvaarding_VZVZ_lang_def.pdf
Kern van het betoog is dat bij gebruik van het LSP (als private doorstart van het eerdere EPD), de aantasting van de privacy van burgers en het beroepsgeheim van de huisarts in het geding zijn.

Enkel het feit dat deze bodemprocedure tegen VZVZ onder behandeling is bij de rechtbank, is relevant voor het bepalen van een “baseline security” en dus relevant bij de herziening van de NEN7512:2005 norm die handelt over de medische informatica, de informatiebeveiliging in de zorg en de vertrouwensbasis voor gegevensuitwisseling. Om die reden richt VPHuisartsen zich nu tot u.

NEN7512:2005 art. 7.4

De huidige NEN7512:2005 norm heeft een rol in de bodemprocedure omdat deze een aantal redelijke, als norm geformuleerde beveiligingsuitgangspunten bevat.
Met name artikel 7.4 ‘Communicatiekanaal en versleuteling’ bevat een aantal sterke voorwaarden voor communicatie tussen twee gebruikers (zorgverleners) die er zorg voor dragen dat aan de

basisvoorwaarden van informatiebeveiliging: Confidentialiteit, Integriteit en Authenticiteit (CIA), wordt voldaan. In het bijzonder om deze eigenschappen *van verzender tot ontvanger* (end to end) te kunnen garanderen. Medische persoonsinformatie wordt, ook vanuit Europese regelgeving, als zeer gevoelig beschouwd en dient zo goed mogelijk beschermd te worden. Daarbij moet de zorgverlener als wettelijk geheimhouder in het bijzonder, als verzender (ontvanger) van informatie, er zeker van kunnen zijn dat confidentialiteit van gegevens tijdens het transport gegarandeerd is. NEN7512:2005 onderscheidt zich doordat deze de CIA voorwaarden vertaalt naar een praktische leidraad die technisch implementeerbaar is.

End-to-end beveiliging

Versleuteling is een basisbegrip bij het elektronisch verzenden van medische gegevens. End-to-end beveiliging (d.w.z. bewaking van authenticiteit, integriteit en confidentialiteit door middel van versleuteling) is een manier waarop het hele communicatiepad van verzender tot ontvanger beveiligd kan worden tegen modificatie of afluisteren van berichten. Bij medische persoonsgegevens – die bij wet beschermd zijn en normaliter alleen voor zorgdoeleinden mogen worden verwerkt – is het evident dat geen ander dan de verzender en de ontvangende partij (zorgverlener) de gegevens mogen inzien en dat de integriteit van de gegevens, en de authenticiteit van verzoeken om informatie, gewaarborgd zijn. Externe partijen – zoals ook VZVZ als verantwoordelijke of beheerders van het LSP – mogen simpelweg geen toegang kunnen krijgen tot medische informatie die tussen zorgverleners wordt uitgewisseld. De technieken om end-to-end beveiliging middels cryptografische technieken mogelijk te maken, zijn reeds lange tijd bekend en relatief eenvoudig implementeerbaar. End-to-end beveiliging vormt daarom een baseline voor de beveiliging van bijzondere persoonsgegevens. Merk op dat in de Zorg-ICT het gebruik van Vecozo- certificaten, UZI-passen en PKIoverheid-certificaten inmiddels gemeengoed is, waardoor aan de technische randvoorwaarden voor end-to-end beveiliging is voldaan. Ook het voor versleuteling benodigde sleutelmanagement hoeft daardoor niet langer een probleem te zijn.

Door VZVZ wordt ten aanzien van het LSP geenszins voldaan aan de eis van end-to-end beveiliging. Hoewel end-to-end versleuteling (confidentialiteit), integriteit en authenticatie al in 2005 in de NEN 7512 norm zijn vastgelegd, blijkt van het gebruik van deze techniek bij het LSP geen sprake te zijn. Tijdens het verzendproces treedt het LSP eerst op als ontvanger van het bericht en bij het verlaten van het LSP weer als zender. De kanalen van en naar het LSP worden versleuteld en geauthenticeerd, echter het kanaal wordt niet van begin tot eind (van *zorgverlener tot zorgverlener* dan wel van *zorgaanbieder tot zorgaanbieder)* beveiligd in de zin van integriteit, authenticiteit en confidentialiteit. Het LSP *moet* aldus volledig vertrouwd worden door de aangesloten zorgaanbieders en indirect door hun patiënten. VPHuisartsen vindt dit model van verondersteld vertrouwen niet vanzelfsprekend, niet noodzakelijk en feitelijk juridisch niet geoorloofd.

(On)versleuteld en translatieservice

Bij verzending van berichten via het LSP stelt VZVZ steevast dat de berichten versleuteld verzonden worden. Door VZVZ wordt echter niet openlijk vermeld dat de medische data gedurende enige tijd onversleuteld de LSP-server passeren.
Ter illustratie: in het businessplan van VZVZ d.d. 01-11-2012 is op twee plaatsen te lezen dat men, middels een translatie(vertaal)-service, binnen de LSP-server van de zogenaamde Professionele

Samenvatting van het HIS een SEH- en een ketenzorgbericht wil kunnen vervaardigen. Het is te vinden in hoofdstuk 4.1.3.3 en 4.1.8.3 van het VZVZ-businessplan.
https://www.vzvz.nl/uploaded/FILES/htmlcontent//Convenant_gebruik_zorginfrastructuur_2013_2016.pdf

Een dergelijke aanpak is uitsluitend mogelijk indien de Professionele Samenvatting tijdelijk onversleuteld op de LSP-server aanwezig is. Uit de AORTA specificatie is ook af te leiden dat end-to-end beveiliging voor het LSP geen ontwerpcriterium is geweest.[1] Dit leidt tot de situatie dat het LSP berichten kan afluisteren, modificeren en injecteren – in tegenspraak met wat zou moeten kunnen, uitgaande van CIA. Er is dus bij gebruik van het LSP *geen sprake van end-to-end beveiliging.*
In het geval van end-to-end beveiliging kan bij aankomst geverifieerd worden of het bericht zich in exact dezelfde toestand bevindt sinds de verzending bij de bron en **nergens** onderweg ontsleuteld is geweest. Zo kan voorkomen worden dat het LSP – en daarmee VZVZ als niet-zorgverlener, of CSC, als beheerder van het LSP, al dan niet in opdracht van derden – gegevens kan opvragen, modificeren of afluisteren.

Patriot Act

De *Patriot Act* houdt al langere tijd de gemoederen bezig. Deze Amerikaanse wet speelt ook een prominente rol in genoemde bodemprocedure. Gezien het feit dat in de LSP-omgeving de data enige tijd onversleuteld voorkomen, is de inhoud van berichten die het LSP passeren zeer kwetsbaar, onder meer voor inzage op basis van de Patriot Act. Er wordt wel gesteld dat inzage door derden op basis van de Patriot Act op grond van Nederlands recht is verboden en dat overtreding tot heroverweging van het contract zal leiden. Iedere kenner van de Patriot Act weet echter dat deze wet een non-disclosure-bepaling kent die het Amerikaanse bedrijf dat mee ***moet*** werken verbiedt om dit openbaar te maken. Ook VZVZ zal niet te weten komen wanneer CSC op basis van de Patriot Act gegevens heeft ***moeten*** opvragen of afluisteren. Het niet voorkomen van correcte end-tot-end-beveiliging heeft daarmee zeer duidelijke consequenties voor de reikwijdte van de Patriot Act bij het LSP. Dit naast het feit dat het LSP behalve NAW-gegevens van patiënten ook informatie over de bij de behandeling van een patiënt betrokken zorgaanbieders kan bevatten, in de verwijsindex en in loggegevens. Daarin zijn opvragingen van specifieke dossiers door specifieke zorgaanbieders te vinden. Dus heeft CSC niet alleen toegang tot gegevens van beschikbare behandelrelaties, maar ook van daadwerkelijke uitgevoerde raadplegingen. Ook dit zijn bijzondere persoonsgegevens in de zin van art. 16 van de Wet bescherming persoonsgegevens (Wbp). Het bedrijf CSC dat het LSP implementeert en onderhoudt, heeft dus inzage in de verwijsindex, de loggegevens en in de inhoudelijke medische gegevens die het LSP-systeem passeren; het laatste is te voorkomen door middel end-to-end beveiliging (versleuteling). Bovendien worden verzoeken om informatie niet geauthenticeerd doorgezet naar goed beheerde zorgystemen (GBZ), waardoor zelfs injectie van verzoeken om informatie zouden kunnen plaatsvinden. Dit raakt aan de basale beveiligingseis van authenticiteit van, in dit geval, opvragingen van gegevens.
Het afwezig zijn van een end-to-end authenticatie, bij het uitwisselen van data over het LS, is een prominent argument in het betoog van VPHuisartsen versus VZVZ. VPHuisartsen stelt in de bodemprocedure op principiële en aan grondrechten en nationale wetgeving ontleende argumenten,

[1] G.J. Van 't Noordende, "A Security Analysis of the Dutch Electronic Patient Record System", Technical report UVA-SNE-2010-01, Universiteit van Amsterdam, 2010.

dat end-to-end beveiliging noodzakelijk is om technisch te voorkomen dat onbevoegden – zoals CSC op basis van de Patriot Act – zich toegang tot medische gegevens *kunnen* verschaffen. Mede vanuit het perspectief dat een zorgverlener het medisch beroepsgeheim moet kunnen garanderen, wat een noodzakelijke voorwaarde is bij het uitwisselen van medische gegevens. Deze garantie kan worden gegeven als wordt voldaan aan de noodzakelijke, technisch en praktisch gezien haalbare en daarom proportionele eis van end-to-end beveiliging.

Wat kan en moet

Bovenstaande toont aan dat het van belang is dat de herziening van de NEN7512:2005 norm op het punt van end-to-end authenticatie, zo goed en zo scherp mogelijk gedefinieerd blijft. En dat de beveiliging die uitgaat van deze norm niet wordt afgezwakt maar sterk en eenduidig blijft. NEN7512:2005 spreekt in hoofdstuk 7.4 heel duidelijk over end-to-end beveiliging. De zender en ontvanger van een bericht ***moeten*** met voldoende zekerheid elkaars identiteit kunnen vaststellen (authenticiteit). Het bericht ***moet*** op geen enkele wijze gewijzigd zijn (integriteit) en de gegevens ***moeten*** geen anderen kunnen bereiken dan de geadresseerde (confidentialiteit). Dit is heldere taal. Dit is, zoals gezegd, ook implementeerbaar, in alle systemen die op dit moment in de markt zijn, van OZIS (in verbeterde vorm) tot het LSP, tot aan IHE-systemen[2]

In de eerder genoemde bodemprocedure refereert VPHuisartsen aan NEN7512:2005 om het principe van end-to-end authenticatie te illustreren. Discussie ontstaat naar aanleiding van de *herziening* van NEN7512:2005 die deze principiële eis bijstelt. Dit geeft aan dat door de herziening van de NEN-norm tijdens de bodemprocedure, de NEN Commissie 303006 als actor in deze procedure terecht komt. De vraag is of de commissie dit heeft voorzien of wenselijk acht.

Afzwakking van de norm

Bij lezing van de conceptherziening van NEN7512:2005 kan VPHuisartsen zich niet aan de indruk onttrekken dat de bestaande norm wordt afgezwakt. Het meest kritieke punt hierbij is het genoemde artikel 7.4, 'Communicatiekanaal en versleuteling'. In de conceptherziening is het hoofdstuk over de elektronische berichtenuitwisseling ondergebracht in punt 6.3.4. VPHuisartsen constateert dat daarin de eisen betreffende communicatiekanaal en versleuteling neerwaarts zijn bijgesteld en minder strak gedefinieerd ten opzichte van NEN7512:2005. Het lijkt erop dat daarmee de situatie met betrekking tot het LSP wordt vergoelijkt of gelegitimeerd. Er wordt in de herziene norm slechts gesproken over het versleutelen op *segmenten* van het kanaal. Als voorbeeld wordt aangehaald dat encryptie alleen van toepassing is tussen de koppelvlakken aan de buitenkant of rand van de infrastructuur van partijen. Dit is zeker niet hetzelfde als end-to-end beveiliging zoals beschreven in NEN7512:2005. End-to-end wordt wel genoemd maar slechts als onderdeel van een onduidelijke zin in relatie tot een kanaal van het publieke Internet tot een '*exclusief, niet-toegankelijk en end-to-end bewaakt, fysiek medium'*. Ook dit slaat niet op een situatie waarin de verzender (zorgverlener A) zeker wil zijn dat alléén de ontvanger (zorgverlener B) het bericht kan inzien en de authenticiteit kan worden vastgesteld. De oorspronkelijke, heldere en eenduidige definities uit NEN7512:2005, artikel 7.4, die basale end-to-end garanties met betrekking tot CIA eigenschappen beschrijven, zijn verdwenen. Wanneer bijzondere persoonsgegevens worden uitgewisseld via een netwerk of via een systeem dat

[2] IHE: Integrating the Healthcare Enterprise, www.ihe.net

niet onder directe verantwoordelijkheid van een zorgverlener valt, volstaan de definities van de herziene norm niet.

State of the art

Indien de herzieningscommissie als motief voor deze wijziging zou aanvoeren dat de in NEN7512:2005 vastgelegde end-to-end verplichting in de praktijk niet overal gebruikt wordt en *daarom* niet haalbaar lijkt te zijn en dat men daarom de huidige praktijk volgt, gaat zij in de ogen van VPHuisartsen voorbij aan de verplichting die zij als de commissie heeft een norm te stellen die – qua beveiliging – '*state of the art'* is. Verantwoordelijken voor gegevensuitwisseling, in het bijzonder van medische gegevens, moeten conform de wet (i.h.b. de Wbp) de best mogelijke beveiliging gebruiken die gegeven de huidige stand van techniek mogelijk is. De huidige NEN7512:2005 geldt al sinds 2005. Door de toenmalige auteurs werd end-to-end beveiliging al mogelijk geacht en deze wordt in de beveiligingswereld ook al lange tijd als 'state of the art' beschouwd.[3,4,5] Het veld had zich al lang moeten – en kunnen – aanpassen aan de eisen die deze norm stelt. Dat dit niet gebeurd is, is als kwalijk en nalatig te kwalificeren en het zou niet beloond moeten worden met neerwaartse bijstelling van de norm.

Beveiligingsexperts

Naar aanleiding van de ledenlijst van de projectgroep, vermeld op pagina 3 van het herzieningsvoorstel, willen wij het volgende onder uw aandacht brengen. Er zijn meerdere veldpartijen vertegenwoordigd, zoals NPCF, VECOZO, EZDA, Zorgring-NHN, HL7 en NICTIZ, een tweetal ziekenhuizen en een aantal adviseurs uit de zorgsector.
Het had in de rede gelegen VPHuisartsen uit te nodigen als veldpartij die zich in rechte inspant voor veilige zorgcommunicatie, om mee te denken over de herziening van NEN7512:2005. Verder valt op dat, hoewel commissieleden op het gebied van Zorg-ICT, datacommunicatie en beheer van zorgcomputersystemen werkzaam zijn, er geen uitgesproken beveiligingsexperts bij betrokken zijn. Dit lijkt ons, gegeven de inhoud van de norm, wel een essentiële voorwaarde. Wij achten het daarom van belang en stellen voor de samenstelling van de herzieningscommissie aan te passen om zo te waarborgen dat deskundige beveiligingsexperts meedenken over de conceptherziening van NEN7512:2005.
Een alternatief zou kunnen zijn om een evaluatiecommissie met onafhankelijke beveiligingsexperts in te stellen die de conceptnorm kan evalueren en waar nodig corrigeren op punten die raken aan onder meer de geheimhoudingsplicht van zorgverleners of andere aspecten die de beveiliging van zorgcommunicatie raken. VPHuisartsen zou graag gekend worden in de samenstelling van een dergelijke evaluatiecommissie of van een aangepaste herzieningscommissie.

Uitspraak bodemprocedure

Het zal duidelijk zijn dat de bodemprocedure die VPHuisartsen voert tegen VZVZ, van invloed kan zijn op de herziening van de NEN7512:2005 norm. In de bodemprocedure wordt gesteld dat end-to-end beveiliging mogelijk en – primair vanuit juridisch maar ook ethisch perspectief - noodzakelijk is bij de

---

[3] A.S. Tanenbaum and M. Van Steen, "Distributed Systems – Principles and Paradigms, 2nd Ed., Pearson Prentice Hall, 2007
[4] R. Anderson, "Security Engineering", 2nd. Ed., Wiley, 2008. (1st editie: 2001).
[5] B. Schneier, "Applied Cryptography", 2nd Ed., Wiley, 1996.

uitwisseling van medische gegevens tussen zorgverleners. Het lijkt dan ook onverstandig en voorbarig op dit moment een definitief besluit te nemen over de conceptherziening van de NEN7512:2005 norm.
De uitkomst van de bodemprocedure kan immers zijn dat de rechtbank stelt dat end-to-end-beveiliging tussen opvragende en bevraagde zorgaanbieder zowel 'state of the art' is - want met beschikbare techniek uitvoerbaar -, als noodzakelijk.

Overigens is VPHuisartsen van mening dat, *ongeacht* de uitkomst van de procedure, artikel 7.4 van de NEN7512:2005 norm in stand gehouden zou moeten worden. Wij achten het onaanvaardbaar een NEN-norm, die tot doel heeft een baseline normering te vormen voor beveiliging van gegevensuitwisseling, neerwaarts wordt bijgesteld. In het bijzonder waar het om medische gegevens gaat wenst VPHuisartsen een beveiliging op een adequaat en ten opzichte van de huidige situatie, hoger nivo dat voldoet aan NEN7512:2005.

In het licht van bovenstaande opmerkingen adviseert VPHuisartsen de tekst van de conceptherziening van NEN 7512:2005, te heroverwegen en/of de uitkomst van de bodemprocedure van VPHuisartsen versus VZVZ af te wachten.
Het dringende advies van VPHuisartsen om zo snel mogelijk beveiligingsexperts te betrekken bij de revisie van NEN7512:2005, blijft uiteraard overeind.

Wij ontvangen graag binnen 14 dagen uw reactie op dit schrijven. Wij zien uw visie met betrekking tot zowel de verdere herzieningsprocedure als de aangedragen inhoudelijke punten, graag tegemoet. Indien verduidelijking of aanvullende informatie nodig is naar aanleiding van ons commentaar, zijn wij uiteraard te allen tijde bereid hierover met u te communiceren.

Met vriendelijke groet,

Bestuur VPHuisartsen W. N. van den Berg, voorzitter J.C. Nobel, secretaris

cc de heer Piet-Hein Daverveldt, directeur NEN
de heer drs. Kees van der Waaij, bestuursvz. NEN