Bijlage Bb (hoort bij Bijlage B) - Normering informatiebeveiliging Landelijk EPD

V1.0

(NB: de nummers in de tabel verwijzen naar de opmerkingen onder de tabel)

Component infrastructuur	Verantwoordelijke	NEN 7510	NEN 7511 1	NEN 7512 2	NEN 7513	Audit (onder wiensverantwoordelijkheid, intern/extern, onafhankelijkheid, frequentie)
LSP	VVZ	X	X	X3	X	Zie opmerking 8
ZSP (datacommunicatie-netwerk)	zorgaanbieder4	X5	X		n.v.t.6	Zie opmerking 9
Informatiesysteem zorgaanbieder	zorgaanbieder	X7	X		X	Zie opmerking 10

Opmerking 1: NEN 7510 en 7511 zijn inmiddels samengevoegd in de NEN 7510:2011.
Opmerking 2: De NEN 7512 richt zich op het vertrouwen tussen de bij de uitwisseling betrokken partijen en de technische maatregelen die nodig zijn om het juiste vertrouwensniveau tussen de partijen te bereiken. Om deze reden is de NEN 7512 van toepassing op de *keten* van componenten en verantwoordelijken en is deze kolom ook als zodanig ingevuld, in plaats van voor de componenten afzonderlijk.
Opmerking 3: De NEN 7512 vereist een inschatting van het risiconiveau van communicatie. Dit risiconiveau is (overigens conform de in de AV23[1] opgenomen richtlijnen) ingeschat op risiconiveau 'hoog'. Hieruit zijn, zoals aangegeven in NEN 7512, de bestaande eisen voor authenticatiemiddelen en versleuteling afgeleid. De UZI-pas voldoet aan de hoogste eisen voor authenticatiemiddelen. Bij uitwisseling via de AORTA-infrastructuur wordt de verbinding versleuteld. Daarnaast kan voor berichten gebruik worden gemaakt van een elektronische handtekening. Risicobeoordelingen vinden jaarlijks intern plaats en architectuurkeuzes worden op grond daarvan zonodig bijgesteld.
Opmerking 4: De zorgserviceprovider (ZSP) in het AORTA-model is de leverancier van het datacommunicatie-netwerk dat het GBZ verbindt met het LSP. De ZSP is een toeleverancier van de zorgaanbieder (GBZ-eigenaar) en opereert daarmee onder diens verantwoordelijkheid. In de zin van de NEN 7510 valt de zorgserviceprovider onder de regels voor externe partijen (hoofdstuk 6.2 van de NEN7510:2011, respectievelijk hoofdstuk 6.2.3 – beveiliging in overeenkomsten met een derde partij).
Opmerking 5: De zorgserviceprovider (ZSP) valt *indirect* onder de NEN 7510 in de zin dat de ZSP een toeleverancier is van de zorgaanbieder/GBZ-eigenaar. De ZSP opereert onder verantwoordelijkheid van de zorgaanbieder.
Opmerking 6: De zorgserviceprovider (ZSP) is de netwerkleverancier. Bij het transport van de informatie over het netwerk van de ZSP is de verbinding tussen GBZ en LSP volledig versleuteld, waardoor geen toegang bestaat tot de inhoudelijke

[1] G.W. van Blarkom en drs. J.J. Borking; *Beveiliging van persoonsgegevens - Achtergrondstudie en verkenning nr. 23*; Registratiekamer, April 2001

informatie die nodig zou zijn voor logging volgens NEN 7513. Deze logging vindt plaats op de eindpunten, dus bij LSP en GBZ.
Opmerking 7: De verantwoordelijke voor het LSP gaat op basis van de bestaande wetgeving uit van de eigen verantwoordelijkheid van de zorgaanbieders om te voldoen aan de NEN 7510.
De zorgaanbieder zelf is verantwoordelijk voor het organiseren van audits op dit gebied, conform het gestelde in de NEN 7510 in hoofdstuk 6.1.8 (onafhankelijke beoordeling van informatiebeveiliging). Omdat de eisen in de NEN 7510 zich uitstrekken tot de volledige organisatie van de zorgaanbieder, moet specifiek voor de aansluiting op het LSP de brede set van eisen uit de NEN 7510 praktisch worden toegespitst op het onderdeel van informatieuitwisseling tussen GBZ en LSP. Dit is gedaan door het opstellen van een pakket van 'GBZ-eisen' . Hierin is opgenomen dat de zorgaanbieder aan de NEN 7510 voldoet (zie echter ook opmerking 10). Verder zijn specifieke organisatorische en technische eisen opgenomen die zich toespitsen op de voor de informatie-uitwisseling relevante zaken.
Opmerking 8: In opdracht van Nictiz vindt er jaarlijks een audit plaats door KMPG op basis van de LSP-eisen en NEN 7510. De uit deze audits voorkomende bevindingen worden bij het verantwoordelijke team/organisatie neergelegd en actief bewaakt door de security officer. Hiernaast is de LSP-leverancier contractueel verplicht ISO 27001 gecertificeerd te zijn. Daarnaast zijn en worden regelmatig (jaarlijks) indringertests ("hackertests") uitgevoerd op het LSP en specifiek op nieuwe componenten van de AORTA/LSP infrastructuur. Deze hackertests worden uitgevoerd in opdracht van Nictiz en zijn in het verleden uitgevoerd door: Fox-IT, Madison Gurkha en ISSX. Daarnaast is in 2010/2011 in opdracht van VWS een grootschalige indringertest (hackertest) uitgevoerd op de diverse onderdelen en koppelpunten van de AORTA-infrastructuur. Hierbij zijn XIS-leveranciers, GBZ'en, ZSP's en het LSP betrokken.
Opmerking 9: De ZSP's worden bij het uitkomen van een nieuwe versie van de AORTA-ZSP-eisen verplicht zich te (her)kwalificeren voor deze nieuwe eisen. Deze ZSP-kwalificaties worden uitgevoerd door twee externe partijen, te weten BDO en Duijnborgh. Het verkrijgen/behouden van deze ZSP-kwalificatie is voor de ZSP's een voorwaarde om aangesloten te worden/blijven op de AORTA-infrastructuur.
Opmerking 10: De GBZ-eisen zijn verdeeld in systeemtechnische eisen en beheermatige eisen. De systeemtechnische eisen worden door Nictiz getoetst tijdens zogenaamde 'XIS-kwalificaties', waarbij het zorginformatiesysteem van een leverancier wordt gecontroleerd op het voldoen aan de systeemtechnische eisen (de lijst van XIS-gekwalificeerde leveranciers is te vinden op de Nictiz-website). De beheermatige eisen zijn van toepassing op het zorginformatiesysteem zoals dat door de leverancier voor een specifieke zorgaanbieder is geïmplementeerd. Hierover geeft de GBZ-eigenaar (de zorgaanbieder) een eigen verklaring af, die steeksproefgewijs wordt getoetst tijdens zogenaamde 'schouwingen'. Deze schouwingen worden uitgevoerd door externe partijen. Bij deze schouwingen wordt getoetst hoe de GBZ'en de eisen hebben ingevuld door een controle op locatie. Op basis van de GBZ-eisen is door Nictiz in overleg met de externe partijen een kader opgesteld voor de schouwingen. Hierin komen onderdelen van de NEN 7510 aan de orde, evenals de omgang met authenticatiemiddelen (NEN 7512) en de logging (NEN 7513).