Whitepaper

Aanbevelingen voor de toepassing van Informatiebeveiligingsnormen in het zorginkoopproces

Auteur: Beer Franken
(lid van normcommissie 303 006: 'Informatievoorziening in de zorg')

0 Voorwoord

Als je met een auto op de openbare weg wilt rijden, moet je een geldig rijbewijs hebben. Maar niemand stelt natuurlijk de vraag of de fabrikant van die auto in het bezit is van een rijbewijs.

Vreemd dus dat iets dergelijks wel vaak gebeurt bij het inkopen van IT-producten- en/of diensten in de zorg. Ziekenhuizen bijvoorbeeld moeten zich houden aan een aantal normen op het gebied van informatiebeveiliging die eisen stellen aan de organisatie, processen en systemen die in het ziekenhuis gebruikt worden. Het gebeurt echter vaak dat diezelfde ziekenhuizen die eisen doorzetten naar de leveranciers van de IT-producten of -diensten die deze processen mogelijk maken.

De hierboven beschreven situatie doet zich dus vaak voor in het inkoopproces van zorgaanbieders. Het blijkt dat met name in dat proces de eis om aantoonbaar te voldoen aan informatiebeveiligingsnormen vaak ongeclausuleerd wordt doorgezet naar de IT-aanbieders. Terwijl die normen primair bedoeld zijn voor de inkopende zorgaanbieders zelf. Vaak liggen onwetendheid over en complexiteit van beleid, wetgeving en normen, hieraan te grondslag. De IT-aanbieder wordt geacht die eisen dan maar zo goed mogelijk te adresseren, zonder de precaire relatie met de eventuele klant op het spel te zetten.

Vanwege deze problematiek organiseerde de normcommissie ‘Informatievoorziening in de zorg’ op 10 oktober 2019 een ontbijtsessie waarin verschillende sprekers op het hierboven geschetste dilemma ingingen. De uitkomsten van die ontbijtsessie vormen de basis voor de aanbevelingen in deze whitepaper.

Dit document beoogt duidelijkheid te bieden aan partijen die betrokken zijn bij het inkoopproces. Hoe zijn de verantwoordelijkheden verdeeld? Welke eisen kan een zorgaanbieder wel ‘doorschuiven’ en welke niet. Wat kunnen zorgaanbieders redelijkerwijs verlangen van hun leveranciers als het gaat om aantoonbaar voldoen aan de belangrijkste NEN Informatiebeveiligingsnormen en wat moeten ze zelf doen?

De normcommissie ‘Informatie voorziening in de zorg’ hoopt met de aanbevelingen in deze whitepaper meer duidelijkheid te scheppen over de toepasbaarheid en toepasselijkheid van de bekendste NEN normen met betrekking tot informatiebeveiliging. En zo te voorkomen dat aan ‘autofabrikanten om rijbewijzen’ wordt gevraagd.

1 Onderwerp en toepassingsgebied

Deze whitepaper doet aanbevelingen over op welke wijze NEN 7510, NEN 7512, NEN 7513 en NTA 7516 moeten worden gehanteerd in het inkoopproces van IT-producten en -diensten voor gebruik in de zorgsector.
De richtlijn is bedoeld voor alle betrokkenen in dergelijke inkoopprocessen.

2 Leeswijzer

Na een overzicht van het juridisch kader in hoofdstuk 3 behandelen de hoofdstukken 4, t/m 8 de belangrijkste NEN normen op het gebied van informatiebeveiliging in de zorg. In elk hoofdstuk wordt beschreven wat de betekenis is van de norm binnen het inkoopproces. Er volgt per norm een aanbeveling over wat een inkopende zorgaanbieder redelijkerwijs mag verwachten van een potentiele leverancier van IT-diensten. In deze aanbevelingen wordt verschillende malen het begrip betekenisloos gebruikt. In hoofdstuk 9 wordt dit begrip kort toegelicht.

Daarna volgt nog een verwijzing naar genoemde bronnen en gebruikte afkortingen.

In het laatste hoofdstuk is meer informatie te vinden over de op 10 oktober 2019 door NEN-normcommissie georganiseerde ontbijtsessie waarin verschillende sprekers op het hierboven geschetste dilemma ingingen. De uitkomsten van die ontbijtsessie vormen de basis voor de aanbevelingen in deze whitepaper.

3 Schets juridisch en normenkader

Zorgverleners zijn wettelijk verplicht zich aan de normen NEN 7510 en 7512 te houden. In artikel 2 van de «Regeling gebruik burgerservicenummer in de zorg» [BSN-Z] staat:

> De gegevensverwerking, bedoeld in de artikelen 8 en 9 van de wet [gebruik burgerservicenummer in de zorg], in artikel 9.1.1, vierde lid, van de Wet langdurige zorg, in artikel 86, eerste, vierde en vijfde lid, van de Zorgverzekeringswet en in de artikelen 28, tweede lid, en 29 van het Besluit gebruik burgerservicenummer in de zorg voldoet aan de NEN 7510[, NEN 7511 en NEN 7512].

Vaak worden ICT-leveranciers van zorgverleners gevraagd (of gedwongen) ook aan NEN 7510, NEN 7512 en NEN 7513 te voldoen. Het BOZ-model verwerkersovereenkomst [BOZ] verwoordt het als volgt:

> [...]
> 4.2 Verwerker werkt aantoonbaar in overeenstemming met ISO 27001 en/of NEN 7510 [...].
> 4.3 Verwerker voldoet aantoonbaar aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN 7512.
> 4.4 Verwerker voldoet aantoonbaar aan de eisen ten aanzien van logging zoals beschreven in NEN 7513.
> 4.5 Verwerker voldoet aantoonbaar aan de eisen van andere NEN-normen voor zover die voor de gezondheidszorg van toepassing zijn verklaard.
> [...]

De Algemene Inkoopvoorwaarden Gezondheidszorg (AIVG) van de NEVI en een aantal zorgkoepels stelt in de ICT module [NEVI]:

> 2.1 De beveiliging dient doeltreffend te zijn met het oog op de stand van de techniek en de gevoeligheid van de gegevens. [...] Hiernaast staat Leverancier er voor in dat hij zal blijven voldoen aan de geldende regelgeving op het gebied van informatiebeveiliging in de zorg. Hier wordt in ieder geval onder verstaan: NEN 7510, 7511, 7512 en 7513.

Het is te verwachten dat zorgleveranciers ook de recent gepubliceerde NTA 7516-eisen aan IT-leveranciers willen opleggen.

In de volgende hoofdstukken wordt aangegeven op welke wijze NEN 7510, NEN 7511, NEN 7512, NEN 7513 en NTA 7516 moeten worden gebruikt in het inkoopproces van IT-producten en -diensten voor gebruik in de zorgsector. In hoofdstuk 4 wordt ingegaan op de verschillende soorten leveranciers met betrekking tot NEN 7510. In hoofdstuk 5 wordt de situatie rond NEN 7512 kort besproken. Hoofdstuk 6 heeft betrekking op NEN 7512 in relatie tot verschillende soorten IT-leverancier. In hoofdstuk 7 wordt de positie van IT-leveranciers ten opzichte van NEN 7513 besproken. In hoofdstuk 8 wordt de situatie rond NTA 7516 geschetst en in hoofdstuk 9 wordt aangegeven wat de gevolgen zijn van zogenaamd ‘betekenisloze’ eisen.

4 NEN 7510

4.1 Doelgroep van NEN 7510

'NEN 7510 geeft richtlijnen en uitgangspunten voor het bepalen, instellen en handhaven van maatregelen die zorginstellingen en andere beheerders van persoonlijke gezondheidsinformatie moeten treffen ter beveiliging van de informatievoorziening'.[1]

Omgekeerd is NEN 7510 niet bedoeld voor partijen (zoals leveranciers) die geen persoonlijke gezondheidsinformatie beheren. Echter, sommige dienstverleners (service providers) beheren wel persoonlijke gezondheidsinformatie, waardoor NEN 7510 op hen wel van toepassing is.

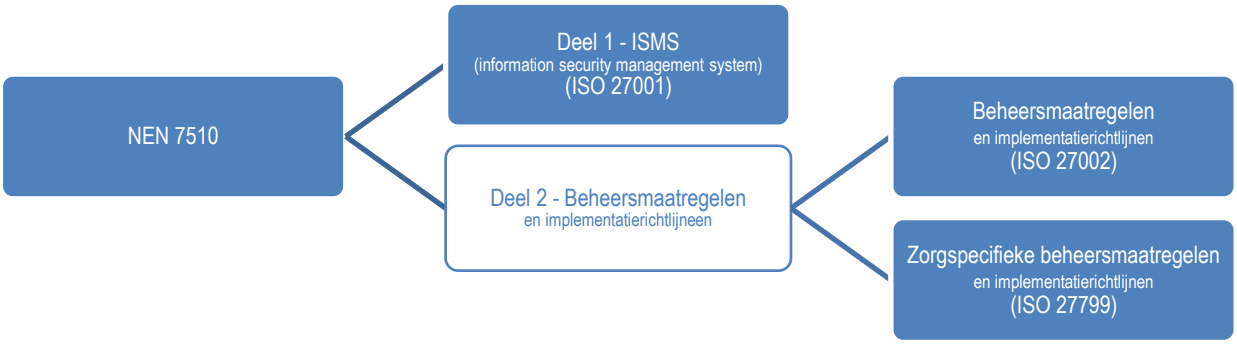
Opmerking 1 Voorbeeld van een dienstverlener die persoonlijke gezondheidsinformatie beheert is een bedrijf dat rechtstreeks ten behoeve van patiënten/cliënten een PGD (persoonlijk gezondheidsdossier) voert: de leverancier beheert in opdracht van de patiënt/cliënt. Of een leverancier van een cloud-gebaseerd medisch dossiersysteem ten behoeve van een huisarts: de leverancier beheert in opdracht van die huisarts.

Opmerking 2 Voorbeeld van een dienstverlener die geen persoonlijke gezondheidsinformatie beheert is de leverancier van software waarmee een ziekenhuis zelf haar EPD (elektronisch patiëntendossier) voert: het ziekenhuis beheert de persoonlijke gezondheidsinformatie zelf.

4.2 Naleving van NEN 7510 door leveranciers

Als aan een leverancier, die geen persoonlijke gezondheidsinformatie beheert, wordt gevraagd om NEN 7510 na te leven (of naleving ervan aan te tonen), dan geldt het volgende.

NEN 7510-1 gaat in op het zogenaamde information security management system (ISMS) en komt overeen met ISO 27001. NEN 7510-2 behandelt beheersmaatregelen die moeten worden overwogen en komt overeen met die van ISO 27002, aangevuld met de beheersmaatregelen van ISO 27799. Met andere woorden:



1 Eerste alinea paragraaf 1.1 van NEN 7510.

Als een organisatie NEN 7510 naleeft, dan leeft deze bijgevolg ook de mondiale norm ISO 27001/2 na. Andersom geldt dat niet. In NEN 7510-2 staan de aanvullende beheersmaatregelen uit ISO 27799 aangegeven onder kopjes met de naam 'Zorgspecifieke beheersmaatregel'; deze 'Definieert de zorgspecifieke beheersmaatregel zoals genoemd in [...] ISO 27799 [...], om, ingeval zorggegevens worden verwerkt of bewerkt, aan de beheersdoelstelling te voldoen.'[2]
Naast zorgspecifieke beheersmaatregelen worden in NEN 7510 ook zorgspecifieke implementatierichtlijnen weergegeven: 'Biedt meer gedetailleerde informatie [dan de 'gewone' implementatierichtlijn] om de implementatie van de beheersmaatregel te ondersteunen en om te voldoen aan de doelstelling van de beheersmaatregel.' Zulke implementatierichtlijnen zijn niet toepasselijk voor organisaties waar geen zorggegevens worden verwerkt'[3].

De conclusie is dat wanneer de leverancier geen persoonlijke gezondheidsinformatie beheert en ook niet voor de organisatie beheert, dan verdwijnt het normatieve verschil tussen enerzijds NEN 7510 en anderzijds ISO 27001/2. Naleving van ISO 27001/2 is in die gevallen gelijk aan naleving van NEN 7510.

Wel moet worden opgelet dat het toepassingsgebied van het ISMS, zoals dat blijkt uit de verklaring van toepasselijkheid[4], geen zaken uitsluit die voor de opdrachtgever (de zorginstelling) van belang zijn.

Opmerking Of de verklaring van toepasselijkheid aansluit bij de beoogde situatie moet altijd worden gecontroleerd en is onafhankelijk van naleving van NEN 7510 dan wel ISO 27001/2.

5 NEN 7511

NEN 7511 is in 2011 ingetrokken en bestaat feitelijk niet meer.[5] De eis om NEN 7511 na te leven is daarom betekenisloos.

2 Hoofdstuk 4 van NEN 7510-2

3 Hoofdstuk 4 van NEN 7510-2

4 Clausule 6.1.3 van NEN 7510-1 respectievelijk ISO 27001.

5 https://www.nen.nl/NEN-Shop/Norm/NEN-751112005-nl.htm.

6 NEN 7512

6.1 Doelgroep van NEN 7512

'NEN 7512 heeft betrekking op de elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, met zorgverzekeraars en andere partijen die bij de zorg zijn betrokken'.[6]

Een leverancier van IT-producten of -diensten is geen zorgverlener, zorginstelling, patiënt, cliënt of zorgverzekeraar, maar mogelijk wel zo'n 'andere partij bij de zorg betrokken'.

Het doel van NEN 7512 is dat twee (of meer) partijen die met elkaar in het kader van zorgverlening elektronisch (gaan) communiceren, afspraken met elkaar maken waarmee tussen deze partijen een vertrouwensbasis wordt gebouwd rekening houdend met de risico's die bij de betreffende samenwerking spelen.

6.2 Naleving NEN 7512 door leveranciers

Er zijn twee situaties waarbij een leverancier van IT-diensten en -producten in de zorg in zekere zin kan worden gehouden NEN 7512 na te leven.

— In het eerste geval is de leverancier te zien als een bij de zorg betrokken partij. De eis voor naleving van NEN 7512 moet worden gezien als een uitnodiging om met de inkopende partij tot op NEN 7512 gebaseerde afspraken te komen. De reactie van de leverancier mag door de inkopende organisatie niet als afwijzingsgrond of lagere waardering van het aanbod van de leverancier worden geïnterpreteerd.

Opmerking Voorbeeld is een dienst die ECG-signalen classificeert .

— In het tweede geval moet de leverancier een oplossing bieden, die op NEN 7512 gebaseerde afspraken tussen de inkopende zorgpartij en een of meer andere zorgpartijen moet ondersteunen of respecteren. Dan moet de eis van naleving van NEN 7512 worden gezien als een eis dat bestaande, op NEN 7512 gebaseerde afspraken, moet worden gerespecteerd dan wel ondersteund. Een leverancier kan hier echter alleen uitspraak over doen, als hij is geïnformeerd over de geldende afspraken tussen partijen. Als de leverancier niet over die afspraken wordt geïnformeerd, is de eis aan een leverancier tot naleving van NEN 7512 betekenisloos.

Opmerking Voorbeeld is als zorgpartijen hebben afgesproken dat authenticatie moet plaatsvinden op basis van een fysiek bezit van een token en een digitaal certificaat; de oplossing van de leverancier moet dat dan ondersteunen dan wel niet in de weg zitten.

De kern van NEN 7512 is dat twee of meer partijen onderling afspraken maken. Naleving eisen door één partij (bijvoorbeeld een leverancier) is betekenisloos.

6 Tweede alinea van hoofdstuk 1 van NEN 7512.

7 NEN 7513

7.1 Doelgroep van NEN 7513

'NEN 7513 stelt eisen aan de registratie van gegevens rond de toegang tot het elektronisch patiëntdossier bij een zorginstelling of een andere organisatie die persoonlijke gezondheidsinformatie verwerkt'.[7]

7.2 Naleving van NEN 7513 door leveranciers

Als een leverancier geen elektronische persoonlijke gezondheidsinformatie bij of voor een zorginstelling of een andere organisatie die persoonlijke gezondheidsinformatie verwerkt, is de eis aan een leverancier tot naleving van NEN 7513 betekenisloos. Anders zijn er twee situaties waarbij een leverancier van IT-diensten en -producten in de zorg kan worden verlangd NEN 7513 na te leven.

— In het eerste geval gaat het om leveranciers die een systeem hebben ontwikkeld, waarmee persoonlijke gezondheidsinformatie wordt verwerkt door een zorginstelling of andere organisatie. Hun systeem moet in staat zijn om elke toegang tot onderdelen van de persoonlijke gezondheidsinformatie te loggen conform de eisen die de klant moet vastleggen. In dat geval moet de eis van naleving van NEN 7513 worden gezien als een eis dat specifieke NEN 7513-voorwaarden van de klant ondersteunt. Een leverancier kan hier echter alleen uitspraak over doen, als hij is geïnformeerd over die voorwaarden. Als de leverancier niet over die voorwaarden wordt geïnformeerd, is de eis aan een leverancier tot naleving van NEN 7513 betekenisloos.

  Opmerking Voorbeelden van zulke NEN 7513-voorwaarden zijn dat de te loggen gebruikers-ID moet zijn gebaseerd op een LDAP- of AD-identiteit, of welke tabellen voor de te loggen autorisatieprotocollen, behandelrelatieprotocollen en toestemmingsprofielen moeten worden gebruikt, of op welke wijze locatie en bron moeten worden geïdentificeerd.

— In het tweede geval gaat het om leveranciers die een systeem beheren waarmee persoonlijke gezondheidsinformatie wordt verwerkt door een zorginstelling of andere organisatie. Zulke leveranciers moeten zorgdragen voor de juiste uitvoering van het loggen en het beheer van de loggegevens, conform de eisen van de zorginstelling. In dit geval moet de eis van naleving van NEN 7513 worden gezien als een eis tot het naleven van door de klant te specificeren NEN 7513-voorwaarden. Een leverancier kan hier echter alleen uitspraak over doen, als hij is geïnformeerd over die voorwaarden. Als de leverancier niet over die voorwaarden wordt geïnformeerd, is de eis aan een leverancier tot naleving van NEN 7513 betekenisloos.

  Opmerking Voorbeelden van zulke NEN 7513-voorwaarden zijn voorwaarden ten aanzien van de verantwoordelijkheid, beschikbaarheid, toegang tot en bewaartermijnen van de logging.

7 Eerste alinea van hoofdstuk 1 van NEN 7513.

8 NTA 7516

NTA 7516 stelt dat een organisatie, die veilig ad-hoc wil communiceren (bijvoorbeeld via e-mail), criteria moet vaststellen die in de situatie waarin de organisatie handelt, moeten worden gerespecteerd. Een deel van die criteria moet door de organisatie zelf worden geïmplementeerd en nageleefd. Sommige andere delen kunnen door leveranciers van IT-producten en/of -diensten worden verzorgd. (In de praktijk zullen vaak meerdere leveranciers zulke criteria vervullen).[8]
Een eis aan een leverancier dat NTA 7516 moet worden nageleefd, moet daarom worden vergezeld van door de organisatie vastgestelde criteria die – volgens de inkopende organisatie – betrekking hebben op de leverancier. Als de leverancier niet over deze criteria wordt geïnformeerd, is de eis aan een leverancier tot naleving van NTA 7516 betekenisloos.

Opmerking Ongespecificeerd naleving van NTA 7516 door een leverancier verlangen, is betekenisloos. Alleen al omdat het label 'leverancier' op zeer uiteenlopende wijzen kan worden ingevuld: De ene doet alles, de tweede geen mail-clients, de derde alles, maar geen portaalfunctionaliteit, de vierde geen mail-clients én geen portaalfunctionaliteit, de vijfde doet alles maar laat fysieke controleonderdelen van eIDAS over aan de klant, de zesde is juist gespecialiseerd in dergelijke controles etc.

9 Het begrip «betekenisloos»

Als in het inkoopproces een eis aan een leverancier als 'betekenisloos' wordt geclassificeerd, dan houdt dit in dat geen enkele reactie van een leverancier op zo'n eis als afwijzingsgrond of lagere waardering van het aanbod van de leverancier mag worden geïnterpreteerd door een inkopende organisatie.

9 Om die reden eist NTA 7516 dan ook dat leveranciers publiek maken welke criteria in welke mate worden nageleefd.

Bronvermelding en Bibliografie

[BOZ] Model Verwerkersovereenkomst Brancheorganisaties Zorg, vindplaats https://live-nvz-api.pantheonsite.io/sites/default/files/2019-05/Verwerkersovereenkomst-BOZ_181217%20bijlage.pdf [laatst geraadpleegd op 27 oktober 2019]

[BSN-Z] Regeling gebruik burgerservicenummer in de zorg, permalink https://wetten.overheid.nl/BWBR0023923/

ISO 27001 NEN-EN-ISO/IEC 27001:2017 *Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen*

ISO 27002 NEN-EN-ISO/IEC 27002:2017 *Informatietechnologie – Beveiligingstechnieken – Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging*

ISO 27799 NEN-EN-ISO 27799:2016 *Medische informatica – Informatiebeveiligingsmanagement in de gezondheidszorg volgens ISO/IEC 27002*

NEN 7510-1 NEN 7510-1:2017 *Medische informatica – Informatiebeveiliging in de zorg – Deel 1: Managementsysteem*

NEN 7510-2 NEN 7510-2:2017 *Medische informatica – Informatiebeveiliging in de zorg – Deel 2: Beheersmaatregelen*

NEN 7512 NEN 7512:2015 *Medische informatica – Informatiebeveiliging in de zorg – Vertrouwensbasis voor gegevensuitwisseling*

NEN 7513 NEN 7513:2018 *Medische informatica – Logging – Vastleggen van acties op elektronische patiëntdossiers*

[NEVI] Algemene Inkoopvoorwaarden Gezondheidszorg, vindplaats https://nevi.nl/sites/default/new_files/AIVG_2017_module_ICT_28_2_2017.pdf [laatst geraadpleegd op 27 oktober 2019]

NTA 7516 NTA 7516:2019 *Medische informatica – Eisen voor veilige e-mail en chatapplicaties (uitwisseling van ad-hocberichten met persoonlijke gezondheidsinformatie*)

Achtergrond whitepaper: Ontbijtsessie 10 oktober 2019

De NEN normcommissie 'Informatievoorziening in de zorg' organiseerde op 10 oktober 2019 een ontbijtsessie, bedoeld voor ICT-leveranciers en inkopers in de zorg en hun adviseurs op het gebied van informatiebeveiliging. In deze druk bezochte sessie werd de vraag besproken: Wat mogen zorginstellingen nu wel en niet van hun ICT-leveranciers verwachten als het gaat om aantoonbaar voldoen aan NEN 7510, NEN 7512, NEN 7513 en NTA 7516?

Tijdens de sessie[9] werd het dilemma zowel vanuit het perspectief van een IT-leverancier[10] als vanuit het perspectief van de inkoper[11] van een zorgaanbieder toegelicht.

Deze whitepaper moet gezien worden als de uitkomst van de nuttige discussies die volgden. De tekst is namens de normcommissie geschreven door Beer Franken[12], zelfstandig adviseur op het gebied van informatiebeveiliging en gegevensbescherming.

De aanbevelingen in deze whitepaper reflecteren de zienswijze van de normcommissie 303 006 'Informatievoorziening in de zorg'.

Contact & meer informatie

Wilt u op de hoogte blijven van de ontwikkelingen op het gebied van informatievoorziening in de zorg, bent u benieuwd naar de aansluiting op standaardisatie of wilt u uw steentje bijdragen en normcommissielid worden? Neem contact op met Kars Jansen (secretaris van de normcommissie (015 26 90 261 of via zw@nen.nl).

Meer informatie over NEN 7510 en de andere in deze whitepaper genoemde normen vindt u op www.nen.nl/nen7510

[9] De presentaties die tijdens de ontbijtsessie zijn toegelicht, zijn hier terug te vinden.
[10] Robert van Wijk, bestuurslid van OIZ ging in op de probleemstelling, gezien vanuit het blikveld van een ICT-leverancier.
[11] Kees Rietman, vertelde namens het bestuur van NEVI-zorg hoe door een inkoper naar de probleemstelling wordt gekeken.
[12] Naast Beer Franken (Piasau) hebben ook Bianca Brooijmans en Dré Lameir (Enovation), Ben Kokx (Philips) en Kars Jansen (NEN) een bijdrage geleverd.