3030060011 "Revisie NEN 7510"

Ontwerpbesluit elektronische gegevensverwerking door zorgaanbieders

Document type:	Public document
Datum van document:	2016-12-02
Reactie NL:	INFO
Opmerking secretaris:	belangrijke info mbt regelgeving waarin naar NEN 7510, 7512 en 7513 wordt verwezen
E-mailadres secretariaat:	kars.jansen@nen.nl
Commissie webadres:	https://isolutions.iso.org/ecom/livelink/open/42648524

Besluit van

houdende nadere regels over functionele, technische en organisatorische maatregelen bij elektronische gegevensverwerking door en tussen zorgaanbieders (Besluit elektronische gegevensverwerking door zorgaanbieders)

Op de voordracht van Onze Minister van Volksgezondheid, Welzijn en Sport, mede namens de Staatssecretaris van Veiligheid en Justitie, ;

Gelet op artikel 26 van de Wet bescherming persoonsgegevens;

De Afdeling advisering van de Raad van State gehoord (advies van 11 juli 2014, no. W13.14.0125/III);

Gezien het nader rapport van Onze Minister van Volksgezondheid, Welzijn en Sport, van PM, no. PM, uitgebracht mede namens de Staatssecretaris van Veiligheid en Justitie;

Hebben goedgevonden en verstaan:

§ 1. Algemeen

Artikel 1

In dit besluit wordt verstaan onder:
elektronisch uitwisselingssysteem: een elektronisch uitwisselingssysteem als bedoeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
logging: de stelselmatige geautomatiseerde registratie van gegevens bedoeld in artikel 35, tweede lid van de wet en artikel 15e van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg alsmede de bestanden waarin die registratie is opgeslagen;
NEN: een door de Stichting Nederlands Normalisatie-instituut uitgegeven norm;
NEN 7510: norm voor het organisatorisch en technisch inrichten van de informatiebeveiliging in de zorg;
NEN 7512: nadere invulling van NEN 7510 betreffende de veiligheid van gegevensuitwisseling tussen partijen in de zorg;
NEN 7513: nadere invulling van NEN 7510 betreffende het vastleggen van acties op elektronische patiëntdossiers;
wet: Wet bescherming persoonsgegevens;

zorgaanbieder: zorgaanbieder als bedoeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg;
zorginformatiesysteem: elektronisch systeem van een zorgaanbieder voor het verwerken van persoonsgegevens in een dossier als bedoeld in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, niet zijnde een elektronisch uitwisselingssysteem;
zorgserviceprovider: netwerkleverancier van een beveiligde netwerkverbinding tussen een zorginformatiesysteem en een elektronisch uitwisselingssysteem.

Artikel 2

1. De verantwoordelijke voor een elektronisch uitwisselingssysteem benoemt een functionaris voor de gegevensbescherming als bedoeld in artikel 62 van de wet.
2. Een instelling als bedoeld in artikel 1, eerste lid, van de Wet kwaliteit, klachten en geschillen zorg die is aangesloten op een elektronisch uitwisselingssysteem, benoemt een functionaris voor de gegevensbescherming als bedoeld in artikel 62 van de wet.

Artikel 3

1. De verantwoordelijke voor een elektronisch uitwisselingssysteem draagt overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van dat elektronisch uitwisselingssysteem.
2. Een zorgaanbieder draagt overeenkomstig het bepaalde in NEN 7510 en NEN 7512, zorg voor een veilig en zorgvuldig gebruik van het zorginformatiesysteem en een veilig en zorgvuldig gebruik van het elektronisch uitwisselingssysteem waarop hij is aangesloten.
3. De verantwoordelijke voor een elektronisch uitwisselingssysteem werkt met een zorgserviceprovider die is geautoriseerd op basis van overeenkomstig NEN 7512 vastgestelde criteria.
4. Een rechtspersoon, niet zijnde een zorgaanbieder, die een elektronisch uitwisselingssysteem beheert en in stand houdt, voldoet aan de volgende voorwaarden:
a. een van de rechtspersoon onafhankelijke organisatie heeft na onderzoek vastgesteld dat de rechtspersoon en het systeem dat hij beheert voldoen aan het bepaalde in NEN 7510 en NEN 7512 en heeft die bevinding opgenomen in een door die organisatie ten behoeve van de rechtspersoon opgesteld audit-rapport;
b. de rechtspersoon heeft het College bescherming persoonsgegevens de in artikel 27 van de wet voorgeschreven melding gedaan onder overlegging van het in onderdeel a bedoelde audit-rapport dat niet ouder is dan drie maanden;
c. de in onderdeel a bedoelde vaststelling is niet langer dan vijf jaar geleden gedaan.

Artikel 4

Bij het vastleggen van beleid, procedures en verantwoordelijkheden als bedoeld in NEN 7510, NEN 7512 of NEN 7513 in documenten, gebruiken de verantwoordelijke voor een elektronisch uitwisselingssysteem en de zorgaanbieder de termen en definities als genoemd in NEN 7510, NEN 7512 of NEN 7513.

Artikel 5

1. De zorgaanbieder als verantwoordelijke voor een zorginformatiesysteem en de verantwoordelijke voor een elektronisch uitwisselingssysteem dragen er zorg voor dat de logging van het systeem voldoet aan het bepaalde in NEN 7513.
2. Vertegenwoordigende organisaties van zorgaanbieders en patiënten stellen, in overleg met het College bescherming persoonsgegevens, overeenkomstig het bepaalde in NEN 7513 de bewaartermijn voor logging vast en maken die bewaartermijn bekend in de Staatscourant binnen 6 maanden na de inwerkingtreding van dit besluit. Indien niet binnen deze termijn een bewaartermijn bekend is gemaakt, stelt de Minister een bewaartermijn vast en maakt die bekend in de Staatscourant.

Artikel 6

De zorgaanbieder als verantwoordelijke voor een zorginformatiesysteem en de verantwoordelijke voor een elektronisch uitwisselingssysteem, vergewissen zich steeds van de laatste stand van de wetenschap en techniek met betrekking tot informatiebeveiliging en de bescherming van persoonsgegevens, en verantwoorden zich over de toepassing daarvan bij de inrichting en het gebruik van hun systemen.

Artikel 7

Voor de uitvoering van dit besluit wordt toepassing gegeven aan de laatste uitgave van de genoemde NEN. Onze Minister van Volksgezondheid, Welzijn en Sport doet van een nieuwe uitgave van NEN, mededeling in de Staatscourant. Bij die mededeling wordt bekend gemaakt op welke datum de nieuwe uitgave van toepassing wordt, waarbij onderscheid kan worden gemaakt tussen bestaande en nieuwe elektronische uitwisselingssystemen en zorginformatiesystemen.

Artikel 8

Het Besluit gebruik burgerservicenummer in de zorg wordt als volgt gewijzigd:
1. Artikel 1 wordt als volgt gewijzigd:
a. Onderdeel a komt te luiden:
a. *wet*: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.
b. Onderdeel k vervalt.
2. Artikel 2, derde en vierde lid vervalt.

Artikel 9

1. Dit besluit treedt in werking op het tijdstip dat de wet van PM houdende wijziging van de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens) in werking treedt.
2. Na inwerkingtreding van de wet bedoeld in het eerste lid berust het Besluit gebruik burgerservicenummer in de zorg op de artikelen 2, 11, 15, 17 en 17a van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de artikelen 17 en 21, vierde lid, van de Wet algemene bepalingen burgerservicenummer.

Artikel 10

Dit besluit wordt aangehaald als: Besluit elektronische gegevensverwerking door zorgaanbieders.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Minister van Volksgezondheid,
Welzijn en Sport,

E.I. Schippers

De Staatssecretaris van Veiligheid en Justitie

K.H.D.M. Dijkhoff

NOTA VAN TOELICHTING

ALGEMEEN DEEL

1. Aanleiding voor deze algemene maatregel van bestuur

Met de verwerping door de Eerste Kamer op 5 april 2011 van het wetsvoorstel houdende nadere regelgeving omtrent infrastructuur en inrichting van een landelijk EPD (kamerstukken I, 2010/2011 31 466. Nr. A), heeft de Eerste Kamer tevens een motie aangenomen van het lid Tan c.s. (kamerstukken I, 2010/2011 31 466 Y), waarin de regering werd verzocht om:

"*te komen tot een nadere wettelijke regeling van normen en standaarden voor zowel digitale dossiervorming en ontsluiting, als de overdracht van gegevens, eisen met betrekking tot veiligheid, toezicht, handhaving en sanctie, inzage door de patiënt, het verstrekken van afschrift aan de patiënt en transport van gegevens van de patiënt, teneinde veilig digitaal transport van gegevens (zowel pull als push) mogelijk te maken tussen zorgverleners binnen een regio*".

Naar aanleiding van deze motie is een juridische analyse uitgevoerd, waarbij bezien is in hoeverre bestaande wetgeving aangepast dient te worden met het oog op veilige en betrouwbare elektronische gegevensuitwisseling in de zorg (kamerstukken II, 2010/2011, 27 529, nr. 82). Uit deze juridische analyse komt naar voren dat de huidige regelgeving op een aantal punten aanpassing behoeft, omdat deze onvoldoende toereikend is, dan wel het maatschappelijk gewenst is iets extra's te regelen. Dit doet zich onder andere voor met betrekking tot het stellen van specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling in zijn algemeenheid. Op grond van het bepaalde in artikel 26 Wet bescherming persoonsgegevens (Wbp) wordt thans in deze amvb een nadere uitwerking gegeven aan de motie Tan c.s., meer in het bijzonder wat betreft toepasselijke normen en standaarden met betrekking tot de overdracht en de veiligheid van de elektronische gegevensuitwisseling.

2. Juridisch kader

2a. Toepasselijke normen en standaarden

Artikel 13 Wbp verplicht de verantwoordelijke om "*passende technische en organisatorische maatregelen ten uitvoer te leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen*".

In de memorie van Toelichting bij de Wbp wordt opgemerkt dat in het begrip "*passend*" besloten ligt dat de beveiliging van persoonsgegevens in overeenstemming is met de stand van de techniek en voorts dat er sprake is van proportionaliteit tussen de beveiligingsmaatregelen en de te beschermen gegevens. "Naarmate de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke

levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er moet sprake zijn van een adequate beveiliging”[1].

Op grond van het bepaalde in artikel 26 Wbp kunnen voor een bepaalde sector bij algemene maatregel van bestuur nadere regels worden gesteld voor de in de artikelen 6 tot en met 11 Wbp en artikel 13 Wbp geregelde onderwerpen.

Van deze zeer ruime delegatiegrondslag is tot op heden geen gebruik gemaakt voor het stellen van nadere regels ten behoeve van de bescherming van persoonsgegevens. Dit besluit geeft uitwerking aan de beveiligingsplicht van artikel 13 Wbp van zorgaanbieders en andere organisaties die bij de informatievoorziening in de gezondheidszorg betrokken zijn. Aangezien de Staatssecretaris van Veiligheid en Justitie eerstverantwoordelijk is voor de Wbp, is hij mede betrokken geweest bij de totstandkoming van dit besluit.

Voor de informatiebeveiliging in de zorg zijn normen beschikbaar van het Nederlands Normalisatie-instituut, te weten NEN 7510:2011 (NEN 7510) en de verdere uitwerking van deze algemene norm betreffende informatiebeveiliging in de zorg in NEN 7512 en NEN 7513. Naar deze normen wordt in deze amvb dwingend verwezen. Dit betekent dat wanneer een zorgaanbieder de in NEN 7510 en overige genoemde normen aangegeven maatregelen heeft getroffen, er van uit mag gaan dat deze “*passende technische en organisatorische maatregelen*” heeft getroffen, als bedoeld in artikel 13 Wbp[2].

Voor zorgaanbieders geldt in het kader van de verwerking van het burgerservicenummer al de verplichting te voldoen aan NEN 7510, 7511 en 7512. Het voldoen aan deze normen is destijds verplicht gesteld naar aanleiding van het advies van het CBP (sinds 1 januari 2016 in het maatschappelijk verkeer aangeduid als de Autoriteit Persoonsgegevens (AP)) om te zorgen voor eenduidige beveiligingsnormen door dwingend te verwijzen, omdat die normen van belang zijn voor de standaardisatie en samenwerking tussen instellingen en bevorderen de mogelijkheden om goed toezicht te houden op een "passende beveiliging" als bedoeld in artikel 13 Wbp. Ook in het kader van het wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens (kamerstukken 33 509) heeft de AP geadviseerd deze normen dwingend voor te schrijven in deze amvb op grond van artikel 26 Wbp. De Minister van VWS heeft de normen afgekocht zodat de vrije verkrijgbaarheid van de normen is gewaarborgd.

2b. Functionele, technische en organisatorische eisen

Zoals in de voorgaande paragraaf wordt opgemerkt, wordt in deze amvb voor wat betreft de aan elektronische gegevensuitwisseling nader te stellen functionele, technische en organisatorische eisen, verwezen naar de door het Nederlands Normalisatie instituut ontwikkelde normen NEN 7510, NEN 7512en NEN 7513.

NEN 7510 richt zich op zorginstellingen en andere organisaties die bij de informatievoorziening in de gezondheidszorg zijn betrokken, ongeacht de aard en

[1] Kamerstukken II 1997-1998, 25 892, nr. 3, p. 99.
[2] In haar onderzoeksrapport “*Toegang tot digitale patiëntendossiers binnen zorginstellingen*” merkt het College bescherming persoonsgegevens (Cbp, thans AP) op bij de toetsing van beveiligingsmaatregelen van zorginstellingen aan artikel 13 Wbp gebruik te maken van NEN 7510 “*als ijkpunt*”. CBP, Toegang tot digitale patiëntendossiers binnen zorginstellingen, Den Haag, juni 2013, blz. 20. Zie in meer algemene zin ook: CBP, Beveiliging van Persoonsgegevens, CBP Richtsnoeren, februari 2013, blz. 16.

de omvang van het bedrijfsproces van de betreffende instelling of organisaties. NEN 7510 verschaft een kader waarbinnen de verantwoordelijke zorgaanbieders voor hun gegevensverwerking relevante informatiebeveiliging kunnen specificeren, inclusief de daarbij behorende (beveiligings)maatregelen.

Het toepassingsgebied van NEN 7510 omvat de beveiliging van alle typen informatie en informatie-uitwisseling tussen zorginstellingen en andere zorgaanbieders en alle mogelijke vormen waarin de informatie wordt weergegeven, vastgelegd en overgedragen. Om de vereiste borging van vertrouwelijkheid, integriteit en beschikbaarheid van de informatie te kunnen bepalen, is een risicobeoordeling noodzakelijk. In NEN 7510 wordt daartoe een risicoclassificatie uitgewerkt.

NEN 7510 geeft verder aanwijzingen voor het organisatorisch en technisch inrichten van de informatiebeveiliging en verschaft hiervoor een normatief raamwerk in de vorm van een zogeheten "*Information Security Management Systeem*" (ISMS). Door implementatie van het ISMS en de beheersmaatregelen bij elk van de beheersdoelstellingen in deze norm, kan een zorgaanbieder voldoen aan de eisen die in een risicobeoordeling zijn vastgelegd. Deze norm geeft daarmee aanwijzingen voor het organisatorisch en technisch inrichten van de informatiebeveiliging en biedt zo een basis voor vertrouwen in de zorgvuldige informatie voorziening bij en tussen de verschillende organisaties in de gezondheidszorg.

NEN 7512 ziet op de elektronische communicatie in de zorg tussen zorgaanbieders en zorginstellingen onderling, met patiënten, met zorgverzekeraars en andere partijen die bij de zorg betrokken zijn. NEN 7512 verschaft binnen dit toepassingsgebied een verdere invulling van een aantal van de richtlijnen van NEN 7510, meer in het bijzonder wat betreft de veiligheid van gegevensuitwisseling tussen betrokken partijen. NEN 7512 verschaft daartoe een schematische benadering voor het classificeren van communicatieprocessen naar het risico dat zij voor de gezondheidszorg met zich meebrengen en formuleert in dat verband minimale eisen ten aanzien van authenticatie en identificatie. Voor elk van de onderscheiden risicoklassen wordt de minimaal vereiste wijze van authenticatie en de bijbehorende bewijsstukken gegeven.

NEN 7513 is een verdere invulling van NEN 7510 wat betreft de "logging". Logging voorziet in de stelselmatige geautomatiseerde registratie van gegevens rondom de toegang tot het (elektronisch) patiëntdossier, hetgeen controle van de rechtmatigheid van de al dan niet verkregen toegang mogelijk maakt. Vanwege het belang van de integriteit van de gegevens in het elektronisch patiëntdossier en de aanwezigheid van bijzondere persoonsgegevens, is het van belang te allen tijde te kunnen achterhalen wie toegang heeft gehad tot het betreffende patiëntdossier, volgens welke regels toegang is verkregen en welke acties op het patiëntdossier zijn uitgevoerd. NEN 7513 biedt zorgaanbieders aanwijzingen voor het loggen en het gebruik van logging om te voldoen aan wettelijke verplichtingen en levert ontwikkelaars van informatiesystemen een aantal eisen waaraan hun informatiesystemen moeten voldoen. Logging moet voorzien in informatie waaraan belanghebbenden (patiënten, zorgaanbieders en toezichthouders) behoefte hebben. Een belangrijk aspect daarbij is de controle op de rechtmatigheid van de raadpleging. Daarnaast kan analyse van de logging ondersteuning bieden voor het verbeteren van het proces van de toegangscontrole tot de patiëntgegevens.

Voor toegang tot en uitwisseling van patiëntengegevens is een norm in ontwikkeling. Het betreft NEN 7521. Deze norm dient te leiden tot uniforme en veilige gegevensuitwisseling tussen betrokken zorgverleners en zorginstellingen rond de behandeling van een patiënt. Zodra NEN 7521 gepubliceerd wordt, zal worden bezien of opname van deze norm in dit besluit noodzakelijk is.

3 Toezicht en handhaving

Op grond van de Wet bescherming persoonsgegevens is het College bescherming persoonsgegevens (sinds 1 januari 2016 in het maatschappelijk verkeer aangeduid als de Autoriteit Persoonsgegevens (AP)) de toezichthouder voor deze amvb. De handhaving van de in deze amvb genoemde normen zal de AP benaderen vanuit het oogpunt van bescherming van persoonsgegevens.
NEN 7510 heeft betrekking op vertrouwelijkheid, integriteit en continuïteit van de geautomatiseerde informatievoorziening. Voor wat betreft het toezicht op NEN 7510 geldt dat de AP zich in zijn toezichthoudende taak richt op misbruik van persoonsgegevens en daarmee op de onderdelen van de norm die zich richten op de vertrouwelijkheid en de integriteit van de gebruikte systemen.
De integriteit en continuïteit van de geautomatiseerde informatievoorziening zijn randvoorwaarden voor verantwoorde zorg. De IGZ heeft op grond van de Kwaliteitswet zorginstellingen tot taak toezicht te houden op verantwoorde zorg en zal de onderdelen van NEN-normen die hiervoor relevant zijn, in haar toezicht betrekken.
De IGZ en het CBP hebben een samenwerkingsprotocol waarin de afspraken tussen het CBP en de IGZ over de wijze van samenwerking bij het toezicht opgesteld.

Gevolgen voor regeldruk

Dit Besluit heeft geen gevolgen voor de administratieve lasten en nalevingskosten. Zoals beschreven wordt met dit Besluit enkel nadere invulling gegeven aan de veiligheid van gegevensverwerking en -uitwisseling door zorgaanbieders. Dit sluit aan bij de huidige praktijk, waarbij zorgaanbieders nu ook al aan de genoemde NEN-normen moeten voldoen. De verplichting om te voldoen aan NEN-normen 7510, 7511 en 7512 is in het kader van de verwerking van het bsn al geregeld in de Regeling gebruik burgerservicenummer in de zorg. Op grond van de Wbp moeten zorgaanbieders nu ook al loggegevens bijgehouden; die logging moet straks voldoen aan NEN 7513. Deze aanpassingen worden bekostigd uit geoormerkte middelen en hebben geen gevolgen voor de zorgverlening. De NEN-normen zijn afgekocht door het Minister van VWS en zodoende voor zorgaanbieders en beheerders van elektronische uitwisselingssystemen kosteloos verkrijgbaar.

ARTIKELSGEWIJZE TOELICHTING

Artikel 1

Voor de definitie van het begrip "*elektronisch uitwisselingssysteem*" wordt verwezen naar de definitie in de Wet aanvullende bepalingen elektronische gegevensverwerking in de zorg. Het betreft een systeem waarmee zorgaanbieders op elektronische wijze, dossiers, gedeelten van dossiers of gegevens uit dossiers voor andere zorgaanbieders raadpleegbaar kunnen maken, waaronder niet

begrepen een systeem binnen een zorgaanbieder, voor het bijhouden van een elektronisch dossier.
In de definitie van "logging" wordt verwezen naar artikel 35, tweede lid van de Wbp en artikel 15e van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Deze artikelen gaan over het bijhouden van de "logging": de gegevens die bij een bepaalde gebeurtenis chronologisch en elektronisch worden vastgelegd, alsmede de bestanden waarin die gegevens worden opgeslagen, zodat is na te gaan wie op welk moment zich toegang heeft verschaft tot bepaalde gegevens.
De normen waaraan in dit besluit wordt gerefereerd, zijn gedefinieerd zonder publicatiejaar. Op grond van artikel 9 geldt altijd de laatste uitgave en wordt het van kracht worden van een nieuwe uitgave, bekend gemaakt in de Staatscourant.
Omdat het van belang is dat bepaalde technische en organisatorische eisen ook gelden voor het systeem dat zorgaanbieders binnen hun organisatie gebruiken voor het op elektronische wijze bijhouden van patiëntengegevens, is een definitie opgenomen van *"zorginformatiesysteem".*
Voor de definitie van het begrip "*zorgserviceprovider*" is tenslotte aansluiting gezocht bij het gebruik van deze term in de praktijk.

Artikel 2

De Wbp geeft verantwoordelijken de mogelijkheid om in het kader van de informatiebeveiliging over te gaan tot aanstelling van een interne toezichthouder, de functionaris voor de gegevensbescherming (FG). Deze kan bij de beveiliging van persoonsgegevens een belangrijke rol spelen onder meer bij controle op naleving van beveiligingsmaatregelen en bij evaluatie en aanpassing van de beveiliging. Om uitdrukking te geven aan het grote belang dat gehecht wordt aan een adequate en passende beveiliging van elektronische gegevensuitwisseling in de zorg en vooruitlopend op de inwerkingtreding van de Algemene verordening gegevensbescherming, is in artikel 2 vastgelegd dat zowel verantwoordelijken voor een elektronisch uitwisselingssysteem als instellingen als bedoeld in artikel 1, eerste lid Wet kwaliteit, klachten en geschillen zorg moeten werken met een FG. Een instelling is een rechtspersoon die bedrijfsmatig zorg verleent, een organisatorisch verband van natuurlijke personen die bedrijfsmatig zorg verlenen of doen verlenen, alsmede een natuurlijke persoon die bedrijfsmatig zorg doet verlenen.

Artikel 3

In dit artikel wordt aan de verantwoordelijke voor een elektronisch uitwisselingssysteem en aan de zorgaanbieder de eis gesteld dat zij zorgen voor een veilig en zorgvuldig gebruik van hun systemen overeenkomstig het bepaalde in NEN 7510 en NEN 7512. Dit betekent dat zij moeten voldoen aan organisatorische eisen en dat zij ervoor zorg moeten dragen dat de gebruikte systemen voldoen aan de technische eisen. Daarnaast geldt voor de rechtspersonen - niet zijnde de zorgaanbieders zelf - die een elektronisch uitwisselingssysteem beheren en in stand houden dat zij moeten voldoen aan dezelfde eisen. Daarom moet op basis van een onafhankelijk onderzoek vastgesteld zijn dat deze rechtspersonen voldoen aan NEN 7510 en NEN 7512.

Artikel 4

Met het oog op de handhaving door de Autoriteit Persoonsgegevens en omwille

van de uitwisselbaarheid van gegevens tussen zorgaanbieders, de verantwoordelijke voor een elektronisch uitwisselingssysteem en de zorgserviceprovider, is hier voorgeschreven dat daarbij de terminologie van NEN 7510 wordt gebruikt.

Artikel 5

De "logging" en welke gegevens in dat verband moeten worden vastgelegd, is geregeld in artikel 35 Wbp en artikel 15e van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. NEN 7513 specificeert de gebeurtenissen die op grond van voornoemde bepalingen in ieder geval in aanmerking komen voor logging en in een logregel behoren te worden vastgelegd. Gegevens die tenminste bijgehouden dienen te worden om logging mogelijk te maken, zijn:
- de gebeurtenis die plaatsgevonden heeft;
- het tijdstip waarop de betreffende gebeurtenis heeft plaatsgevonden;
- welke cliënt dit betrof;
- wie de betreffende gebruiker van het elektronisch uitwisselingssysteem was die de gebeurtenis heeft laten plaatsvinden; en
- namens welke verantwoordelijke de betreffende gebruiker optrad.
In het eerste lid is vastgelegd dat de verantwoordelijken voor zorginformatiesystemen en voor elektronische uitwisselingssystemen ervoor zorg dienen te dragen, dat de logging van die systemen voldoet aan het bepaalde in NEN 7513.

In het tweede lid van dit artikel wordt wordt bepaald dat vertegenwoordigende organisaties van zorgaanbieders en patiënten, in overleg met het CBP, overeenkomstig het bepaalde in NEN 7513 een bewaartermijn voor loggegevens moeten vaststellen en bekend maken. In paragraaf 8.6 van NEN 7513 wordt opgemerkt dat het in beginsel aan patiënten, zorgaanbieders en toezichthouders is om termijnen overeen te komen voor het bewaren van loggegevens. In een noot bij paragraaf 8.6 van NEN 7513 wordt opgemerkt dat de algemene bewaartermijn van medische dossiers 15 jaar is en dat koppeling van de bewaartermijn van de loggegevens aan die van het patiëntendossier waarop deze betrekking hebben voor de hand ligt. Omdat een bewaartermijn van 15 jaar voor loggegevens gelet op de bulk aan data die dat oplevert op praktische bezwaren kan stuiten wordt het onderling overeen komen van een redelijke bewaartermijn voor loggegevens hier aan de zorgaanbieders verplicht gesteld.

Artikel 6

De technieken in de informatiebeveiliging en de bescherming van persoonsgegevens blijven zich ontwikkelen. Het is daarom van belang dat de verantwoordelijken voor de gebruikte systemen steeds op de hoogte blijven van die nieuwe ontwikkelingen en zo nodig verbeteringen in hun systeem doorvoeren. In dit kader wordt ook wel gesproken van "privacy enhanching technologies" (PET). Bijvoorbeeld de scheiding van gegevens in meerdere domeinen. Het ene domein bevat de persoonsgegevens waarmee iemand te identificeren is en het andere domein bevat de medische gegevens. Dit artikel regelt dat verantwoordelijken steeds bezig moeten zijn met het verbeteren van de informatiebeveiliging en bescherming van persoonsgegevens.

Artikel 7

In dit besluit wordt verwezen naar NEN zonder dat daarbij wordt genoemd welke versie het betreft. In dit artikel is geregeld dat steeds toepassing dient te worden gegeven aan de laatst gepubliceerde versie. In het algemeen deel van de toelichting is genoemd welke versies op het moment dat dit besluit in werking is getreden, van toepassing zijn. Op grond van dit artikel wordt door de Minister van Volksgezondheid, Welzijn en Sport in de Staatscourant mededeling gedaan van een nieuwe uitgave van NEN en vanaf welke datum de nieuwe uitgave van toepassing wordt. Hierbij wordt rekening gehouden met de benodigde implementatietijd die nodig kan zijn om aan wijzigingen in NEN te voldoen.

Artikel 8

Met artikel 8 wordt het Besluit gebruik burgerservicenummer in de zorg (Besluit bsn-z) aangepast op de inwerkingtreding van in artikel 9 van dit besluit genoemde wet. De Wet gebruik burgerservicenummer krijgt met de inwerkingtreding van die wet een nieuwe citeertitel: Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Het Besluit bsn-z hangt onder deze wet. Aangezien de reikwijdte van het Besluit bsn-z – anders dan de wet – niet wijzigt, behoudt dit besluit zijn citeertitel.

Artikel 9

Het tijdstip van inwerkingtreding van dit besluit is gekoppeld aan de inwerkingtreding van de Wet cliëntenrechten bij elektronische verwerking van gegevens (kamerstukken 33 509). Omdat de citeertitel van de Wet gebruik burgerservicenummer in de zorg met de inwerkingtreding van die wet wijzigt in Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, wordt in het tweede lid de gewijzigde grondslag van het Besluit gebruik burgerservicenummer in de zorg vastgelegd.

De Minister van Volksgezondheid,
Welzijn en Sport,

E.I. Schippers