vZVZ

/ Factsheet

Het LSP en de nieuwe privacywetgeving; een stand van zaken

Het Landelijk Schakelpunt (LSP) is een landelijk werkende zorginfrastructuur ten behoeve van elektronische uitwisseling van medische gegevens tussen zorgverleners. In wettelijke termen is het LSP een 'elektronisch uitwisselingssysteem' (art. 1 sub j van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg - Wabvpz). In deze factsheet komt aan de orde welke eisen er door de wet- en regelgeving aan een dergelijk systeem worden gesteld en in welke mate het LSP daaraan voldoet.

Auteur: mr C.D.M. Soeterbroek MHA

1. Algemene kenmerken van het LSP als uitwisselingssysteem

Het Landelijk Schakelpunt (LSP) is een landelijk werkende zorginfrastructuur ten behoeve van elektronische uitwisseling van medische gegevens tussen zorgverleners. Over deze zorginfrastructuur kunnen medische gegevens beveiligd, vertrouwd en betrouwbaar op een gestandaardiseerde manier worden uitgewisseld. AORTA is de architectuur waarop de berichtuitwisseling is gebaseerd. In het LSP is de verwijsindex opgenomen.

Op basis van de vraag van een zorgverlener naar bepaalde medische gegevens van de patiënt zoekt het LSP aan de hand van zijn BSN welke zorgverleners gegevens over hem beschikbaar hebben. De verwijsindex registreert waar patiëntgegevens opvraagbaar zijn (i.e. waar de brondossiers zich bevinden), welke gegevens zijn opgevraagd (medicatiegegevens, professionele samenvatting, ICA-gegevens) en door wie (een zorgverlener).

Het uitwisselen van gegevens, en met name van medische gegevens, is aan strikte wet- en regelgeving gebonden. Alvorens in te gaan op de toepasselijke wetgeving en de mate waarin het LSP daaraan voldoet, wordt een schets van het systeem gegeven aan de hand van de kenmerken van het systeem.

De kenmerken van het LSP zijn:

- **Toestemming.** Medische en persoonsgegevens van patiënten kunnen pas tussen zorgverleners uitgewisseld worden, nadat de patiënt daar uitdrukkelijke en geïnformeerde toestemming voor heeft gegeven aan zijn zorgverlener (opt-in) én deze toestemming is geregistreerd in zowel het zorginformatiesysteem (XIS) van de zorgaanbieder, als in de Verwijsindex van het LSP.
- **Beveiliging.** Uitsluitend zorginformatiesystemen die gekwalificeerd zijn als "Goed Beheerd Zorginformatie-systeem" (GBZ) kunnen aansluiten op het LSP. Dit houdt in dat medische gegevens veilig worden uitgewisseld via een zorginformatiesysteem en een netwerk-leverancier, een zogeheten "Goed beheerd Zorgnetwerk" (GZN). Een GZN is een door VZVZ geaccepteerde marktpartij die een beveiligde verbinding aanbiedt tussen het GBZ van de zorgaanbieder en het LSP. Beide moeten de acceptatietesten van VZVZ met succes hebben afgerond. NB: de term GZN is gelijk aan de term 'zorgserviceprovider' zoals gehanteerd in het Besluit elektronische gegevensverwerking door zorgaanbieders.
- **Besloten netwerk.** De zorginfrastructuur (AORTA) is een op zichzelf staand (besloten) netwerk en staat geheel los van internet.
- **Identificatie.** Toegang tot de zorginfrastructuur is uitsluitend mogelijk na identificatie aan de hand van het UZI-nummer (Unieke Zorgverlener Identificatie) voor zorgverleners (persoon). Patiënten die online toestemming willen geven en/of inzage willen hebben in

de logginggegevens, dienen zich te identificeren middels DigiD met sms-verificatie.

- **Standaarden voor gegevensuitwisseling / proportionaliteit van gegevens.** Het soort gegevens dat uitgewisseld kan worden (huisartswaarneemgegevens, medicatiegegevens en ICA-gegevens) is bepaald door de betrokken beroepsorganisaties: NHG, KNMP. De gegevens zijn naar aard en omvang afgebakend, waarmee wordt beoogd niet meer gegevens uit te wisselen dan die op het moment van opvragen (pull) noodzakelijk zijn voor de behandeling van de patiënt. Ook is precies vastgelegd welke zorgverlener gegevens mag opvragen/inzien.
- **Authenticatie.** UZI-passen worden door het CIBG verstrekt, uitsluitend aan zorgverleners die zorgaanbieder zijn in de zin van de Wabvpz. In deze wet en het daarbij behorende Besluit (AMvB) worden veiligheidseisen gesteld aan de zorginformatiesystemen, zoals de verplichting om te voldoen aan NEN 7510, 7512 en 7513.
- **Autorisatie.** Aan de hand van de informatie op de UZI-pas ziet het LSP erop toe, dat de informatie alleen wordt verstrekt aan zorgverleners die bevoegd zijn om gegevens in te zien en dat alleen die informatie te zien is waarvoor de zorgverlener bevoegd is.
- **Geen dataopslag.** Uitgangspunt van AORTA is dat gegevens niet centraal worden opgeslagen. In het LSP worden dus geen medische dossiers of medische data opgeslagen of bewaard. De data zijn (en blijven) opgeslagen in het XIS van de zorgaanbieder. In de Verwijsindex wordt uitsluitend opgeslagen bij welke zorgaanbieder(s) zich een medisch dossier van een patiënt bevindt. Voor deze functie verwerkt het LSP het BSN.
- **Logging.** Via de zorginfrastructuur worden gegevens (geautomatiseerd) uit die medische dossiers opgevraagd en, versleuteld, tussen zorgverleners uitgewisseld. Elke opvraging wordt gelogd. Patiënten kunnen daarvan via e-mail bericht ontvangen en via de website Volgjezorg.nl zien wie er gegevens heeft opgevraagd.

2. Juridisch kader voor een systeem voor elektronische gegevensuitwisseling in de zorg

2.1. Wet- en regelgeving

VZVZ volgt de wet- en regelgeving op het gebied van elektronische gegevensuitwisseling en gegevensbescherming op de voet en waarborgt dat het LSP daaraan bij voortduring voldoet. Onder regelgeving worden door VZVZ ook richtlijnen van relevante beroepsgroepen en veldnormen verstaan.

Van toepassing op het systeem van elektronische gegevensuitwisseling zijn de volgende wetten:

- Wet bescherming persoonsgegevens (Wbp) en de opvolger van deze wet, de Algemene Verordening Gegevensbescherming (AVG).
- Wet Cliëntenrechten bij elektronische verwerking van gegevens in de zorg (in werking getreden per 1 juli 2017) met de daaruit voortvloeiende wijzigingen in de Wet gebruik burgerservicenummer in de zorg (BSN-z).
  NB: Sinds de inwerkingtreding is de titel van de wet “Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg” (Wabvpz).
- Het bij de “Wet aanvullende bepalingen” behorende “Besluit elektronische gegevensuitwisseling door zorgaanbieders” (in werking getreden per 1 januari 2018).

En onder meer de volgende regelgeving/veldnormen:

- NEN 7510: naleving van deze norm was reeds voorgeschreven door de Wet BSN-z. Naleving van NEN 7510 (en 7512 en 7513) heeft met inwerkingtreding van “Besluit elektronische gegevensuitwisseling door zorgaanbieders” een dwingend karakter gekregen.
- Privacy bij regionale uitwisseling van patiëntgegevens: Handreiking naar aanleiding van bevindingen van het CBP bij twee regionale situaties (KNMG, KNMP, NHG en VHN, september 2010).
- KNMG-richtlijn Omgaan met medische gegevens (KNMG, september 2016).
- Door de beroepsgroepen vastgestelde berichtenstandaarden.

2.1.1. Wet bescherming persoonsgegevens (Wbp) en Algemene Verordening Gegevensverwerking (AVG)

<u>De Wet bescherming persoonsgegevens (Wbp)</u>
De Wbp is van toepassing op de geautomatiseerde verwerking van persoonsgegevens en de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn of worden opgenomen.
De Wbp, en ook haar opvolger de AVG, kent geen verplichting tot elektronische verwerking.

Een persoonsgegeven is ‘elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. Het 'verwerken' omvat elke handeling met betrekking tot de persoonsgegevens, zoals het inzien, opslaan en delen van de gegevens. De normen uit deze wet richten zich grotendeels

tot de ‘verantwoordelijke’ voor de gegevensverwerking. Dit is ‘degene die het doel en de middelen voor de verwerking van persoonsgegevens vaststelt’. De partij die de gegevens van betrokkenen voor door hem vastgestelde doelstellingen vastlegt en bepaalt hoe de verwerking plaatsvindt, is verantwoordelijke voor die gegevensverwerking. Dat kunnen ook meerdere partijen samen zijn. Wanneer een partij de gegevens vastlegt, in opdracht en voor doelstellingen van een ander, treedt zij op als ‘bewerker’ van de gegevens. Dit is bijvoorbeeld aan de orde bij hosting van een database door een derde dienstverlener, die niet zelf mede-verantwoordelijke is.

Niet alleen is de verantwoordelijke degene die de verplichtingen uit de Wbp moet opvolgen, ook is hij het aanspreekpunt voor betrokkenen met betrekking tot de gegevensverwerking en het uitoefenen van zijn rechten. Hij is ook degene die zorgt voor een passende beveiliging.

De Algemene Verordening Gegevensbescherming (AVG)
Op 25 mei 2018 trad de verordening in werking. Hoewel de Wbp ook al was geschreven met het oog op de digitalisering en elektronische gegevensverwerking is de AVG nog meer gericht op gegevensbescherming van persoonsgegevens in het digitale tijdperk.

De AVG is goeddeels een vastlegging van het bestaande privacyrecht gecombineerd met jurisprudentie en best practices. Vele bepalingen bevatten vernieuwingen ten opzichte van de huidige Wbp, juist om beter aan te sluiten bij elektronische gegevensverwerking. En daarbij gaat het niet alleen om de eigen verwerkingen van de verantwoordelijke, maar ook om de manier waarop hij communiceert met medeverantwoordelijken, bewerkers (in de AVG: verwerkers) van data, derden en niet in de laatste plaats de betrokkene die gebruik maakt van digitale communicatie.

De AVG heeft per 25 mei 2018 de Wbp vervangen. De herziening van het Europese privacy framework beperkt zich niet tot de AVG. De nieuwe ePrivacyrichtlijn is al geruime tijd in consultatie. Deze Richtlijn zal de bescherming van persoonsgegevens bij internetgebruik regelen. Deze Richtlijn wordt aangepast met het oog op de nieuwe markt en technische realiteit. Het verbeteren van beveiliging en vertrouwelijkheid van digitale communicatie is daarbij de kern.

De AVG bevat bepalingen die digitale communicatie voorschrijven in het contact met burgers en medeverwerkers. Een voorbeeld daarvan is dat indien een inzageverzoek elektronisch is gedaan, de informatie op elektronische wijze en in een gebruikelijk format worden verstrekt. Ook voor andere verzoeken geldt indien deze elektronisch zijn gedaan, dat zoveel mogelijk elektronisch beantwoord moet worden.

Nieuwe rechten in de AVG zijn het recht op dataportabiliteit en het recht op vergetelheid. Het recht op dataportabiliteit houdt in dat de betrokkene in bepaalde gevallen (namelijk wanneer er sprake is van elektronische gegevensverwerking) het recht heeft om zijn gegevens in een gestructureerde, gangbaar en machine-leesbare vorm te verkrijgen. En dat hij deze mag overdragen aan een andere verantwoordelijke. Als het technisch mogelijk is, heeft de betrokkene het recht de gegevens rechtstreeks te laten doorsturen van de ene naar de andere verantwoordelijke.
Een andere toevoeging aan de rechten is het recht op vergetelheid. Indien de betrokkene hierom verzoekt, dient de verantwoordelijke de persoonsgegevens van deze betrokkene te wissen. Dit strekt ver. De verantwoordelijke moet er dan namelijk voor zorgen, dat de gegevens uit alle systemen verwijderd worden, ook als deze systemen zich bij sub-verwerkers bevinden.

Tot slot worden er in de AVG meer verplichtingen en bevoegdheden aan verwerkers en verantwoordelijken opgelegd c.q. toegekend. Om te voorkomen dat de verwerker een lichter regime zou treffen dan de verantwoordelijke bij dezelfde gegevensbescherming, of de verantwoordelijke de regelgeving ontloopt of niet goed kan uitvoeren, legt de AVG de verwerker zwaardere verplichtingen op. De verant-woordelijke moet de op hem rustende verplichtingen inzake gegevensbescherming eveneens opleggen aan de verwerker(s) die hij inschakelt.

De verantwoordelijke heeft een verantwoordingsplicht opgelegd gekregen. Deze verplichting brengt met zich mee, dat de verantwoordelijke aan moet kunnen tonen, hoe hij de beginselen, zoals die zijn opgenomen in artikel 5 AVG, naleeft. Daarvoor is het nodig, dat de verantwoordelijke betrokkenen informatie verstrekt over de verzameling van gegevens, de betrokkenen toegang geeft tot die gegevens, aangeeft hoe met die gegevens omgegaan wordt, etc. De verant-woordelijke dient maatregelen toe te passen die, door ontwerp en standaardinstellingen, ertoe leiden dat de gegevensbeschermingsbeginselen doeltreffend worden uitgevoerd (privacy by design, privacy by default).

De verantwoordelijke dient aan te tonen dat hij aan deze verplichtingen voldoet, door het in stand houden van een

Verwerkingsregister en het uitvoeren van gegevenseffect-beoordelingen (Privacy Impact Assessments).
In paragraaf 1 van hoofdstuk 2 van de Wbp en in hoofdstuk 2 van de AVG zijn de voorwaarden opgenomen die gelden voor rechtmatige verwerking van gegevens. Hieronder wordt aangegeven welke voorwaarden dat zijn, hoe die binnen het LSP van toepassing is, en de bewijsvoering dat het LSP aan de betreffende bepaling voldoet.

Ondubbelzinnige toestemming van de betrokkene (art. 8 Wbp en art. 6 en 7 AVG)

Toepassing binnen LSP:
Voor een rechtmatige gegevensuitwisseling is nodig dat de toestemming uit vrije wil wordt verleend, voldoende specifiek is en gebaseerd is op voldoende informatie ('informed consent').

Het LSP werkt uitsluitend op basis van opt-in. De zorgverlener is verantwoordelijk voor het vragen van de toestemming en de registratie daarvan. De zorgverlener dient bij het vragen van de toestemming aan de patiënt de folder van VZVZ 'Uw medische gegevens beschikbaar via het Landelijk Schakelpunt (LSP)' te overhandigen. Deze voldoet aan alle eisen van de Autoriteit Persoonsgegevens. Als de patiënt deze informatie heeft gelezen, weet hij:

- Wat er met zijn medische gegevens gebeurt;
- Op welke gegevens de toestemming betrekking heeft;
- Voor welk doel de gegevensuitwisseling plaatsvindt;
- Welke soorten zorgverleners welke gegevens kunnen inzien;
- Wie verantwoordelijk is voor de gegevensverwerking via het LSP.

De patiënt kan zijn toestemming te allen tijde intrekken.

Bewijsvoering:
VZVZ houdt toezicht op de rechtmatige verwerking van toestemmingen door de naleving van de procedure bij zorgverleners te toetsen. Zorgverleners zijn via de gebruiksovereenkomst gehouden tot medewerking aan deze onderzoeken.

Doelbinding (art. 9 Wbp, art. 5 lid 1b AVG)

Toepassing binnen LSP:
VZVZ stelt als verantwoordelijke vast voor welk doel de gegevens worden verzameld: "het bevorderen van de gezondheidszorg door het optreden als Verantwoordelijke in de zin van de Wbp voor de verwerking van (medische) persoonsgegevens in een landelijke verwijsindex ten behoeve van de uitwisseling van de gegevens."

Bewijsvoering: Deze doelbinding is op genomen in artikel 3 van de statuten van VZVZ.

Bewaren van persoonsgegevens (art. 10 Wbp en art. 5 lid 1e AVG)

Toepassing binnen het LSP:
Persoonsgegevens worden niet langer dan noodzakelijk bewaard voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld.

Bewijsvoering:
VZVZ verwerkt op basis van opt-in uitsluitend het BSN. Het BSN wordt opgeslagen in de Verwijsindex. Wanneer de patiënt zijn toestemming intrekt, wordt het BSN verwijderd uit de Verwijsindex. De gegevens worden bewaard zolang de toestemming niet is ingetrokken.

Dataminimalisatie (art. 11 Wbp en art. 5 lid1c AVG)

Toepassing binnen LSP:
Via het LSP worden verschillende categorieën van medische gegevens uitgewisseld: medicatiegegevens, huisartswaarneemgegevens en ICA-gegevens. De reikwijdte van de gegevens dat uitgewisseld wordt, is bepaald door de betrokken beroepsorganisaties als NHG en KNMP.
De gegevens die uitgewisseld worden zijn naar aard en omvang afgebakend, waarmee wordt beoogd niet méér gegevens uit te wisselen dan die op het moment van opvragen noodzakelijk zijn voor de behandeling van de patiënt.

Bewijsvoering:
Berichtenstandaarden (inclusief de medische autorisatie-richtlijnen (HWG, medicatiegegevens en ICA-gegevens).

Beveiliging (art. 13 Wbp en art. 5 lid 1f AVG)

Toepassing binnen LSP:
"De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer 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 te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen."

Bewijsvoering:
VZVZ is NEN 7510:2011 gecertificeerd met als scope: het verwerken van persoonsgegevens via het LSP, via het VZVZ Servicecentrum en via de portalen (ikgeeftoestemming.nl, formulieren.vzvz.nl en portaal.vzvz.nl). Daarnaast werkt VZVZ conform NEN 7512 en NEN 7513.
VZVZ heeft per 1-7-2017 een Functionaris voor de Gegevensbescherming (FG) aangesteld.

Recht op inzage (art. 35 Wbp en art. 15 AVG)

Toepassing binnen LSP:
De patiënt kan online inzien aan welke zorgverlener hij toestemming heeft verleend om gegevens uit te wisselen, en getoond wordt welke zorgverlener, op welke datum, gegevens heeft opgevraagd. Desgewenst kan de patiënten instellen, dat hij een e-mailbericht ontvangt wanneer een zorgverlener via het LSP medische gegevens van de patiënt heeft opgevraagd.

Bewijsvoering:
Via de website Volgjezorg.nl heeft de patiënt online inzage in diens gegeven toestemmingen en de opvragingen die zijn gedaan.

2.1.2. Wet Cliëntenrechten bij elektronische verwerking van gegevens in de zorg en de Wet gebruik burgerservicenummer in de zorg (BSN-z), thans Wabvpz

Per 1 juli 2017 is de Wet cliëntenrechten bij elektronische verwerking van gegevens in werking getreden. De wet regelt de voorwaarden waaronder zorgverleners medische gegevens veilig en elektronisch kunnen uitwisselen met andere zorgverleners. De wet heeft ertoe geleid, dat een aantal andere wetten is gewijzigd (aangescherpt), waaronder de Wet gebruik burgerservicenummer in de zorg (Wet BSN-z). De Wet BSN-z heet sinds de wetswijziging "Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg" (Wabvpz).

Concreet zijn de aanscherpingen:

- De plicht voor de zorgaanbieder om uitdrukkelijke toestemming van de patiënt te verkrijgen voor het uitwisselen van gegevens. Vanaf 2020 dient de patiënt bovendien in staat te kunnen zijn om aan te geven welke gegevens wel of niet door welke (categorieën van) zorgverleners mogen worden ingezien (gespecificeerde toestemming).
- De plicht van de zorgaanbieder om de patiënt informatie te verstrekken over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen en over de werking van het elektronisch uitwisselingssysteem (in werking per juli 2017).
- De plicht van de zorgaanbieder om ervoor te zorgen dat het elektronisch uitwisselingssysteem dat hij gebruikt,

vastlegt wie gegevens beschikbaar heeft gesteld en wie ze heeft ingezien (logging) (treedt in werking in 2020).
- Het recht van de patiënt op een afschrift van zijn dossier, of van de gegevens betreffende deze patiënt die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt. En de plicht van de zorgaanbieder om deze gegevens elektronisch beschikbaar te stellen (het tweede deel van deze bepaling treedt per 2020 in werking).

Hierna wordt aangegeven in hoeverre het LSP voldoet aan de bepalingen uit de Wabvpz.

Gespecificeerde toestemming (art. 15a Wabvpz)

Tekst van de wet:

1. De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselings-systeem, voor zover de zorgaanbieder heeft vastgesteld dat de cliënt daartoe uitdrukkelijk toestemming heeft gegeven.
2. De in het eerste lid bedoelde toestemming betreft gespecificeerde toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt aan te duiden zorgaanbieders of categorieën van zorgaanbieders.
3. De zorgaanbieder stelt gegevens van de cliënt slechts beschikbaar via een elektronisch uitwisselings-systeem, voor zover bij het raadplegen van die gegevens door een andere zorgaanbieder, de persoonlijke levenssfeer van een ander dan de cliënt niet wordt geschaad.

Toepassing binnen LSP en Bewijsvoering:
Art 15a lid 1. Zie hiervoor bij ‘ondubbelzinnige toestemming’: Hoewel het de verantwoordelijkheid van de zorgaanbieders is om de toestemming van de patiënt correct te verkrijgen en te registreren, houdt VZVZ toezicht op de rechtmatige verwerking van toestemmingen door de naleving van de procedure bij zorgverleners te toetsen. Zorgverleners zijn via de gebruiksovereenkomst gehouden tot medewerking aan deze onderzoeken.

Art. 15a lid 2. Dit artikellid treedt in 2020 in werking. Dit betreft de zogenoemde ‘Gespecificeerde toestemming’. Hiervoor is het project GTS opgestart.
Art. 15a lid 3. De beroepsgroepen stellen de informaties-tandaarden vast en zijn verantwoordelijk voor de registratie van patiëntgegevens in hun informatiesysteem. De verplichting om de persoonlijke levenssfeer van een ander dan de cliënt niet te schade bij het raadplegen van gegevens is een reeds bestaande verplichting

Informatieplicht van de zorgaanbieder (art. 15c Wabvpz)

Tekst van de wet:

1. De zorgaanbieder geeft de cliënt informatie over zijn rechten bij elektronische gegevensuitwisseling, de wijze waarop hij zijn rechten kan uitoefenen en over de werking van het elektronisch uitwisselingssysteem dat voor de gegevensuitwisseling wordt gebruikt. Indien nieuwe categorieën van zorgaanbieders aansluiten bij het elektronisch uitwisselingssysteem, of de werking van het elektronisch uitwisselings-systeem anderszins substantieel wordt gewijzigd, informeert de zorgaanbieder de cliënt over deze wijziging alsmede over de mogelijkheid om de gegeven toestemming, bedoeld in artikel 15a, aan te passen of in te trekken.
2. De zorgaanbieder houdt een registratie bij van de op grond van artikel 15a, tweede lid, door cliënten verleende toestemming waarbij wordt aangetekend vanaf welk tijdstip de toestemming van kracht is geworden. Een zorgaanbieder kan deze registratie beschikbaar stellen via het elektronisch uitwisselingssysteem.

Toepassing binnen LSP en Bewijsvoering:
Art. 15c lid 1: met betrekking tot informatie over het elektronisch uitwisselingssysteem (LSP) heeft VZVZ voor zorgverleners een toolkit ontwikkeld. Daarin is informatie (waaronder folders) opgenomen die de zorgaanbieder kan aanbieden aan de patiënt. Ook is de betreffende informatie te vinden op de website van VZVZ.

Op de website is te vinden welke categorieën van zorgaanbieders zijn aangesloten op het LSP.
T.a.v. het informatiesysteem dat een zorgverlener hanteert, geldt dat VZVZ zorgaanbieders desgevraagd ondersteund bij de communicatie richting patiënten, in het geval de zorgaanbieder (de-)fuseert, of van informatiesysteem verandert.

De eis uit artikel 15c lid 2 is opgenomen in de GBZ-eisen. Een zorgaanbieder die aansluit op het LSP, voldoet daarmee aan deze bepaling.

Toelichting:
LSP voldoet aan de eisen van artikel 15c lid 1.
Artikel 15c lid 2 treedt in 2020 in werking.

Inzage en afschrift (art 15d Wabvpz)

Tekst van de wet:

1. Indien de cliënt verzoekt om inzage of afschrift van het dossier van de desbetreffende cliënt, of van de gegevens betreffende deze cliënt die de zorgaanbieder via een elektronisch uitwisselingssysteem beschikbaar stelt, wordt de inzage of het afschrift op verzoek van de cliënt, met redelijke tussenpozen, door de zorgaanbieder op elektronische wijze verstrekt.
2. Bij de afgifte van medicijnen door een apotheker, verschaft de apotheker de cliënt desgevraagd direct op elektronische wijze inzage in zijn medicatiegegevens. Op verzoek van de cliënt worden door de apotheker desgevraagd door de cliënt verstrekte gegevens over het gebruik van zelfmedicatie beschikbaar gesteld via het elektronisch uitwisselingssysteem.
3. De in het eerste en tweede lid bedoelde elektronische inzage, en de in het eerste lid bedoelde elektronische afschriften, worden kosteloos verschaft.

Toepassing binnen LSP en Bewijsvoering:
Dit artikel treedt in 2020 in werking.

Op dit moment hebben patiënten geen toegang tot het LSP. Opvragen van (uitgewisselde) gegevens kan de patiënt uitsluitend doen bij zijn zorgverlener.
In het programma MedMij, waarin ook VZVZ is betrokken, wordt gewerkt aan een oplossing waarmee de patiënt zelf, elektronische inzage in zijn eigen medische gegevens kan verkrijgen, ongeacht bij welke zorgverlener (huisarts, apotheker, medisch specialist e.a.) deze gegevens zijn opgeslagen.

Logging (art. 15e Wabvpz)

Tekst van de wet:
Onverminderd het bepaalde in artikel 35, tweede lid, van de Wet bescherming persoonsgegevens, wordt in een afschrift als bedoeld in artikel 15d, eerste lid, op verzoek van de cliënt opgenomen:
a. wie bepaalde informatie via het elektronisch uitwisselingssysteem beschikbaar heeft gesteld en op welke datum.
b. wie bepaalde informatie heeft ingezien of opgevraagd en op welke datum.

Toepassing binnen LSP en Bewijsvoering:
Dit artikel treedt in 2020 in werking.

Het LSP voldoet reeds aan deze bepaling. Patiënten die toestemming hebben gegeven voor uitwisseling van hun medische gegevens, kunnen deze gegevens, met uitzondering van de datum waarop bepaalde gegevens beschikbaar zijn gesteld, opvragen en printen via de website Volgjezorg.nl.

Toegang tot elektronische uitwisselingssystemen (art 15f Wabvpz)

Tekst van de wet:

1. Een zorgverzekeraar heeft geen toegang tot elektronische uitwisselingssystemen.
2. Voor zover een zorgaanbieder werkzaamheden verricht als bedrijfsarts, verzekeringsarts, dan wel als keurend arts voor keuringen als bedoeld in de Wet op de medische keuringen, verschaft hij zich geen toegang tot elektronische uitwisselingssystemen en verwerkt geen gegevens uit elektronische uitwisselingssystemen.

Toepassing binnen LSP en Bewijsvoering:
Zorgverzekeraars, bedrijfsartsen, verzekeringsartsen en keuringsartsen hebben geen toegang tot het LSP. De nieuwe wet brengt daarin dus geen wijziging.

Wettelijke vertegenwoordiging (art. 15g Wabvpz)

Tekst van de wet:
Indien de cliënt een wettelijk vertegenwoordiger heeft, worden de op grond van deze paragraaf aan de cliënt toekomende rechten uitgeoefend door deze vertegenwoordiger, met dien verstande dat in afwijking van artikel 5 van de Wbp, toestemming voor het verwerken van persoonsgegevens als bedoeld in de Wbp, mede is vereist van de cliënt die de leeftijd van twaalf maar nog niet van zestien jaren heeft bereikt, tenzij de desbetreffende cliënt niet in staat kan worden geacht tot een redelijke waardering van zijn belangen ter zake.

Toepassing binnen LSP en Bewijsvoering: In het geval er door een ouder/voogd toestemming wordt gegeven voor uitwisseling van gegevens van een kind tussen 12 en 16 jaar, dient het kind het toestemmingsformulier mede te ondertekenen. De nieuwe wet brengt daarin derhalve geen wijziging.

Verantwoordelijkheid voor melding aan de AP van overtreding van art 15f (art. 15h Wabvpz)

Tekst van de wet:
De verantwoordelijke, bedoeld in de Wbp, voor een elektronisch uitwisselingssysteem, doet in geval van een vermoeden van een overtreding van het verbod, bedoeld in artikel 15f, eerste lid, mededeling aan de zorgautoriteit, bedoeld in de Wet marktordening gezondheidszorg.

Toepassing binnen LSP en Bewijsvoering:
VZVZ is verantwoordelijke in de zin van de Wbp/AVG voor het LSP. Zorgverzekeraars hebben (en krijgen ook in de toekomst) geen toegang tot het LSP.

In het voorgaande is aangegeven op welke wijze het LSP voldoet aan verplichtingen ten aanzien van toestemming, informatievertrekking en de wijze waarop de patiënt kan volgen aan wie hij toestemming heeft gegeven en wie op welk moment (zijn) medische gegevens heeft opgevraagd.

Het effectief en efficiënt aanbieden van de mogelijkheid om gespecificeerde toestemming te geven is niet realistisch zonder een elektronische inrichting daarvan. Om de gespecificeerde keuzes te kunnen effectueren is een elektronische koppeling tussen de toestemming en een uitwisselingssysteem onontbeerlijk.
Een traject om gespecificeerde toestemming elektronisch in te regelen is inmiddels gestart (programma GTS).
Een traject om patiënten elektronisch inzage te geven in de eigen medische gegevens is eveneens inmiddels gestart (programma MedMij).

2.1.3. Besluit elektronische gegevensuitwisseling door zorgaanbieders

Aanvullend aan de Wabvpz worden er in de AMvB “Besluit elektronische gegevensuitwisseling door zorgaanbieders” (stb 2017, 446) specifieke functionele, technische en organisatorische eisen aan elektronische gegevensuitwisseling gesteld. Deze AMvB is op 1 januari 2018 in werking getreden.

De AmvB verwijst voor wat betreft de aan elektronische gegevensuitwisseling nader te stellen functionele, technische en organisatorische eisen, dwingend naar NEN 7510, NEN

7512 en NEN 7513. De reden hiervoor is dat 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. Overigens gold voor zorgaanbieders al in het kader van de wet BSN-z de verplichting te voldoen aan NEN 7510, 7512 en 7513.

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

Besluit (AmvB) elektronische gegevensuitwisseling door zorgaanbieders

In het kort moet aan de volgende zes verplichtingen worden voldaan:

1. Art. 2 lid 1: het benoemen van een functionaris voor de gegevensbescherming;
2. Art. 4: het vastleggen van het beleid, de procedures en verantwoordelijkheden rondom gebruikte elektronische uitwisselingsystemen en interne zorginformatiesystemen conform de eisen uit NEN 7510, 7512 en 7513;
3. Ervoor zorgdragen dat gebruikte elektronische uitwisselingssystemen en interne zorginformatiesystemen voldoen aan de veiligheidseisen en zorgvuldigheidseisen van NEN 7510;
4. Ervoor zorgdragen dat overeenkomsten tussen zorgaanbieder en de verantwoordelijke van een elektronisch uitwisselingssysteem voldoen aan NEN 7510;
5. Ervoor zorgdragen dat gebruik wordt gemaakt van veilige verbindingen die voldoen aan NEN 7512;
6. Ervoor zorgdragen dat de logging van patiëntengegevens voldoet aan NEN 7513

Toepassing binnen LSP en bewijsvoering:

- VZVZ is in mei 2017 NEN 7510:2011 gecertificeerd met als scope: het verwerken van persoonsgegevens via het LSP, via het VZVZ Servicecentrum en via de portalen (ikgeeftoestemming.nl, formulieren.vzvz.nl en portaal.vzvz.nl).
- VZVZ werkt conform NEN 7512 en 7513.
- Per 1 juli 2017 is bij VZVZ een Functionaris Gegevensbescherming aangesteld.

Meer informatie

Met vragen of voor meer informatie kunt u contact opnemen met het Servicecentrum:
E-mail: support@vzvz.nl
Telefoon: 070 - 317 34 92 (bereikbaar op maandag t/m vrijdag van 9.00 - 17.00 uur).

Versie: 4 april 2019