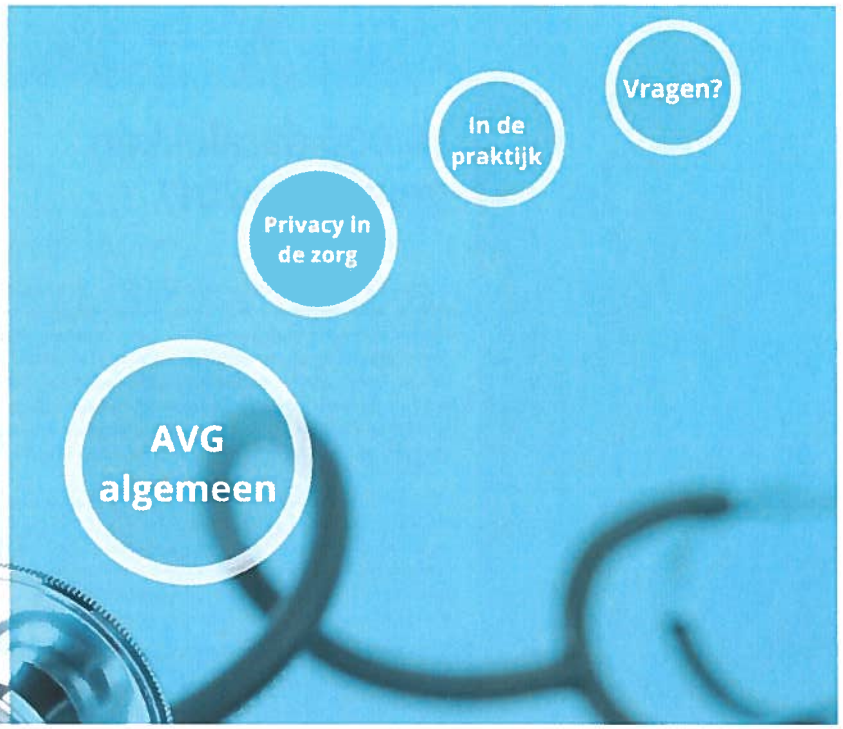
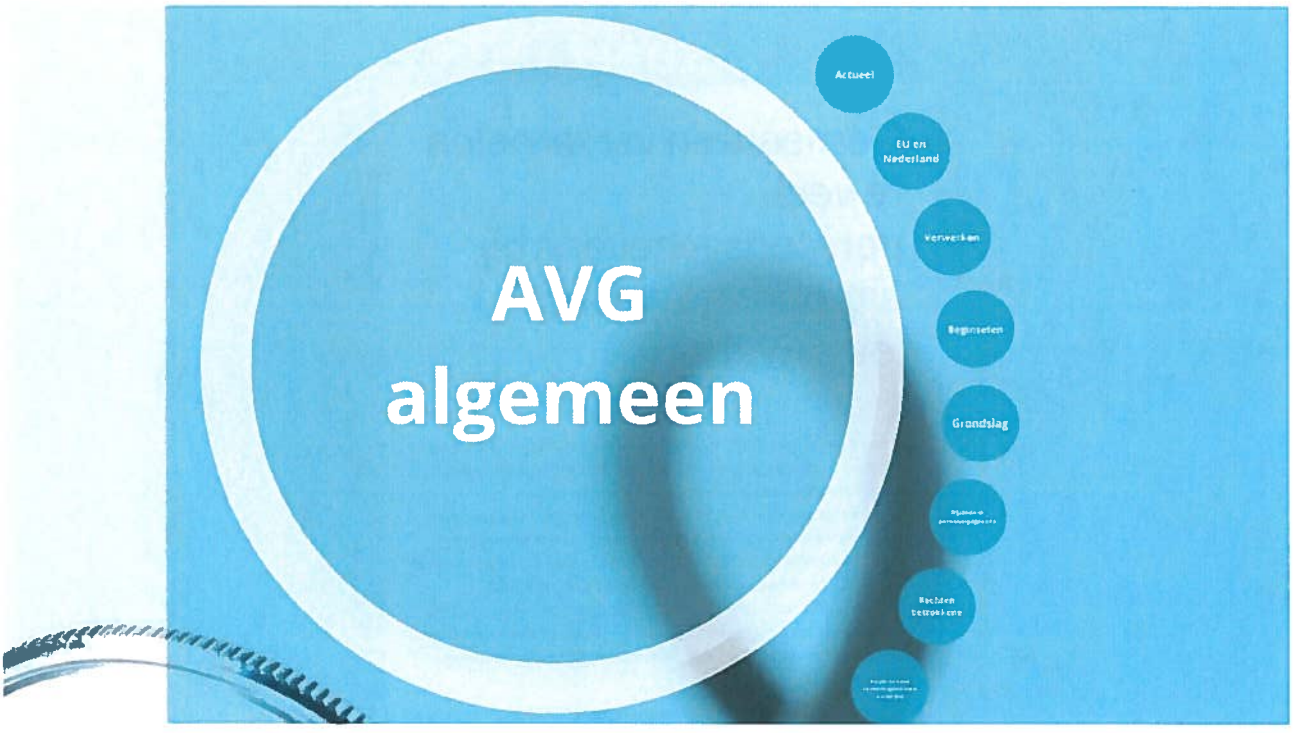
PRIVACY IN DE ZORG EN DE AVG

KBS ADVOCATEN

Niels van den Burg
Erik Luijendijk

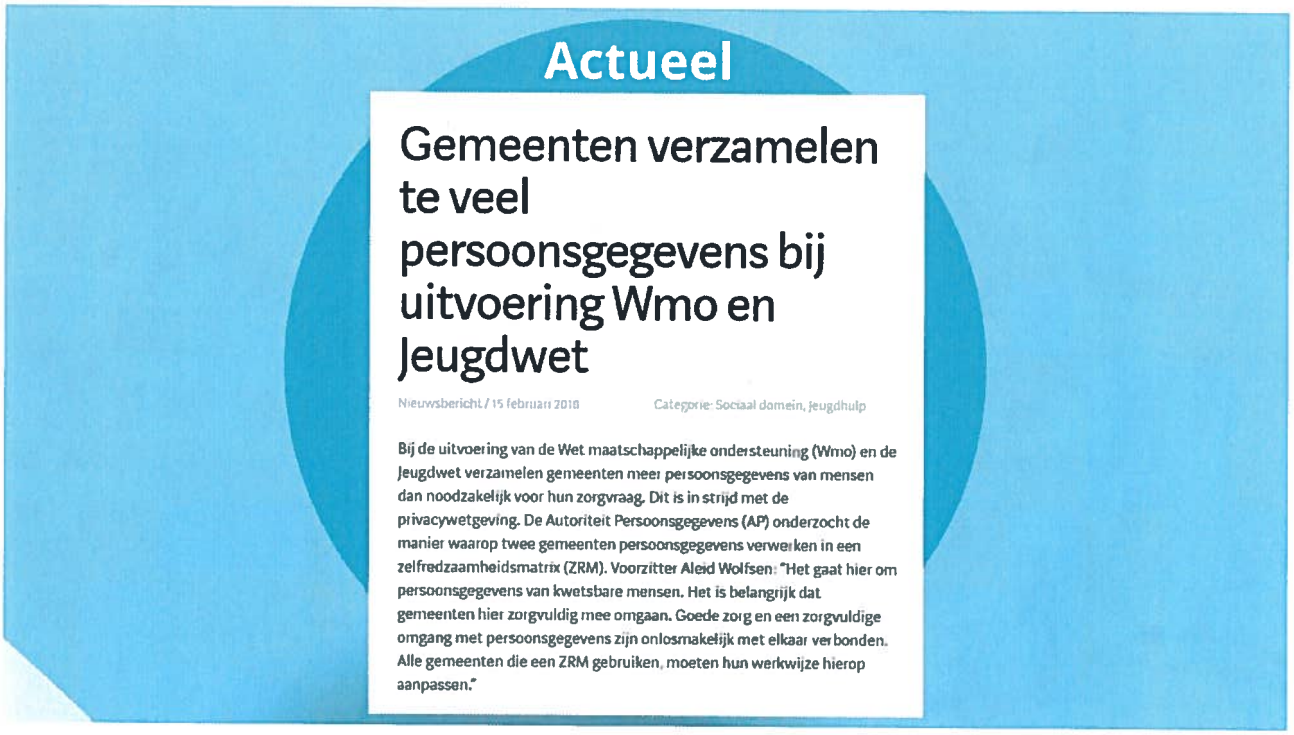


1.



2.


Actueel
10.000 datalekken gemeld in 2017
Nieuwsbericht / 29 maart 2018
Categorie: Meldplicht datalekken
In 2017 zijn 10.000 datalekken gemeld bij de Autoriteit Persoonsgegevens (AP). Het aantal meldingen is in 2017 met ruim 70% toegenomen ten opzichte van het jaar ervoor, van 5849 naar 10.009. De meeste datalekken werden gemeld door organisaties uit de sectoren zorg en welzijn, openbaar bestuur en financiële dienstverlening. Voorzitter Aleid Wolfsen: "We zien een flinke toename van het aantal gemelde datalekken. Het lijkt er enerzijds op dat de bekendheid van de meldplicht toeneemt. Anderzijds baart het ons zorgen dat de beveiliging nog vaak niet op orde is."
Bij bijna de helft van de datalekken (47%) die in 2017 zijn gemeld, gaat het om persoonsgegevens die aan een verkeerde ontvanger zijn gestuurd. Meldingen van kwijtgeraakte persoonsgegevens door bijvoorbeeld een verloren of gestolen laptop, usb-stick of tas met dossiers vormen 15% van het totale aantal gemelde datalekken. Het gaat in de meeste gevallen om NAW-gegevens, geslacht, geboortedatum en BSN.


Actueel
Gemeenten verzamelen te veel persoonsgegevens bij uitvoering Wmo en Jeugdwet
Nieuwsbericht / 15 februari 2018
Categorie: Sociaal domein, Jeugdhulp
Bij de uitvoering van de Wet maatschappelijke ondersteuning (Wmo) en de Jeugdwet verzamelen gemeenten meer persoonsgegevens van mensen dan noodzakelijk voor hun zorgvraag. Dit is in strijd met de privacywetgeving. De Autoriteit Persoonsgegevens (AP) onderzocht de manier waarop twee gemeenten persoonsgegevens verwerken in een zelfredzaamheidsmatrix (ZRM). Voorzitter Aleid Wolfsen: "Het gaat hier om persoonsgegevens van kwetsbare mensen. Het is belangrijk dat gemeenten hier zorgvuldig mee omgaan. Goede zorg en een zorgvuldige omgang met persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Alle gemeenten die een ZRM gebruiken, moeten hun werkwijze hierop aanpassen."

Actueel

05 april 2018

Uit eigen onderzoek van het HagaZiekenhuis is gebleken dat enkele tientallen medewerkers onrechtmatig in een patiëntendossier hebben gekeken. Het HagaZiekenhuis is hiervan geschrokken, want het hecht zeer groot belang aan het waarborgen van de privacy van patiënten. Patiënten moeten er op kunnen vertrouwen dat alleen bevoegde medewerkers hun dossier raadplegen.

De behandelaar heeft de patiënt om wie het gaat geïnformeerd en excuses gemaakt namens het ziekenhuis. Tegen betreffende medewerkers worden disciplinaire maatregelen genomen. Zekerheidshalve is ook de Autoriteit Persoonsgegevens geïnformeerd. Het onderzoek is half maart gestart en zal naar verwachting half april zijn afgerond.

Om de privacy te waarborgen hanteert het ziekenhuis duidelijke gedragsregels op het gebied van informatiebeveiliging. Die zijn ook bekend bij medewerkers. Zij worden hierover vanaf hun indiensttreding geïnformeerd. Zij tekenen ook voor geheimhouding in hun arbeidscontract. Daarnaast zijn hulpverleners gebonden aan de geheimhoudingsplicht op grond van de Wet BIG. Ook zijn zij gebonden aan de Wet Geneeskundige Behandel Overeenkomst (WGBO), die bepaalt dat alleen bevoegde functionarissen patiëntendossiers mogen raadplegen van de patiënten die ze behandelen.

Beleid informatiebeveiliging

Het HagaZiekenhuis houdt permanent alle login-gegevens bij van medewerkers die patientendossiers raadplegen. Dat is conform het beleid van Informatiebeveiliging volgens de NEN 7513. Het ziekenhuis controleert periodiek of dossiers door bevoegde medewerkers worden geraadpleegd. In geval van twijfel wordt zorgvuldig onderzoek ingesteld. Hierbij wordt hoor- en wederhoor toegepast. Indien blijkt dat ten onrechte een dossier is geraadpleegd, wordt een disciplinaire maatregel opgelegd.

Actueel

Datalek in het Erasmus MC

Het Erasmus MC-Sophia heeft bij de Autoriteit Persoonsgegevens melding gemaakt van een datalek.

Mailadressen

Het gaat om een nieuwsbrief van de afdeling Kinderinfectieziekten/Immunologie, die is verspreid in een besloten groep van ouders van patiënten en patiënten van 18 jaar en jonger. De mailadressen van de patiënten zijn per abuis in de To-adressering terechtgekomen, in plaats van in het BCC-veld.

Bezwaard

Er is sprake van een menselijke vergissing, waar de afdeling zich zeer bezwaard over voelt. Ze weten immers hoe gevoelig de privacy ligt. Dit had niet mogen gebeuren, aldus de verklaring van de afdeling. Met de patiënten is dan ook direct nadat de fout aan het licht kwam, contact opgenomen.

Actueel

Autoriteit Persoonsgegevens lekte per ongeluk namen van personeel

Gepubliceerd 16 maart 2018 10 19
Laatste update 16 maart 2018 11 12

De Autoriteit Persoonsgegevens, waarbij bedrijven datalekken verplicht moeten melden, heeft zelf per ongeluk de namen van werknemers openbaar gemaakt.

Dat vertelt onderzoeker Mischa van Geelen van beveiligingsbedrijf NFIR aan NU nl

"Het is niet ons beleid om namen van medewerkers inzichtelijk te maken", aldus woordvoerder Pauline Gras van Autoriteit Persoonsgegevens Daarom worden schrijvers van onderzoeken, wetsadviezen en verslagen nooit openbaar gemaakt.

De namen waren echter te zien in de metadata van pdf-bestanden, waardoor ze alsnog inzichtelijk waren "Die informatie was openbaar in te zien en daarom toegankelijk voor iedereen", vertelt van Geelen

De persoonsgegevens waren te achterhalen bij ongeveer 800 documenten die

EU en Nederland

Fundamentele rechten

- EVRM
- IVBPR
- Handvest Grondrechten EU
- VWEU
- Grondwet

Privacyrechten (25 mei 2018)

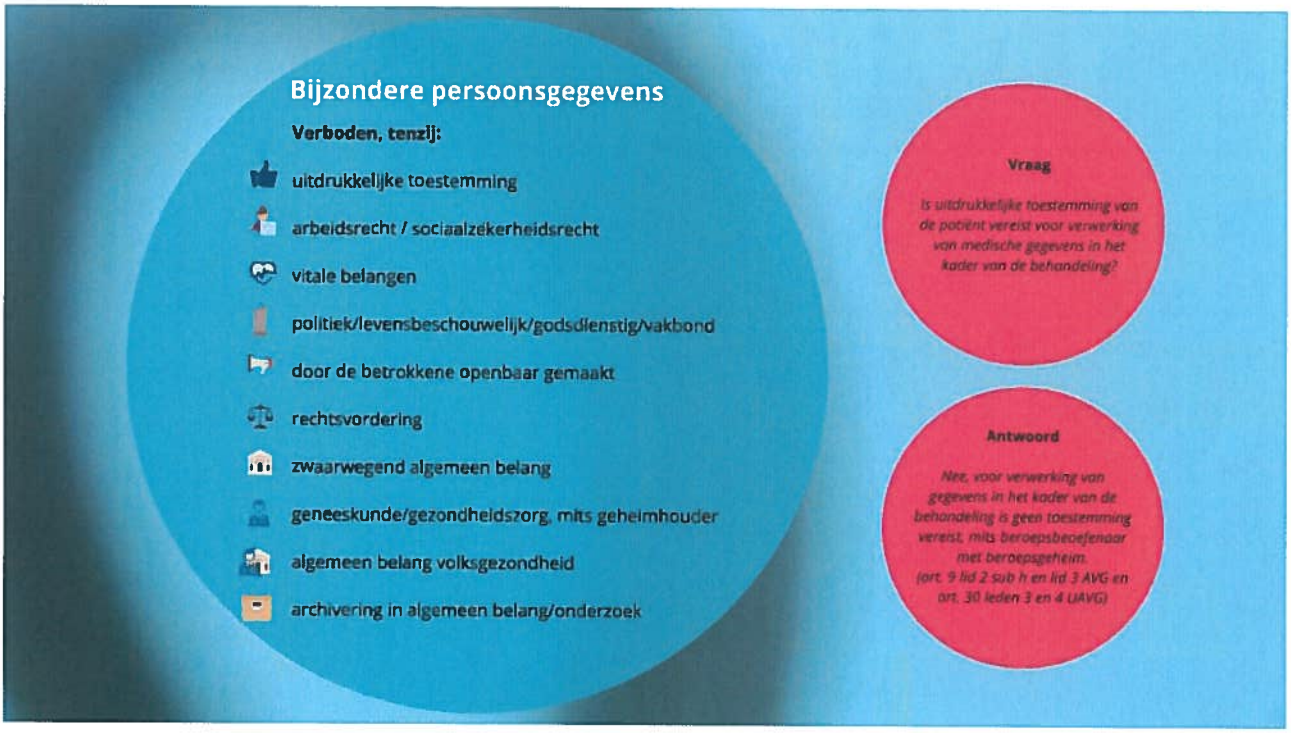
- AVG
- *EU Privacyrichtlijn 95/46/EG*
- *voorstel E-Privacyverordening*
- Uitvoeringswet AVG
- *Wbp*


Verwerken
Verwerken: *ruime definitie*
Persoonsgegevens: *identificatoren herleidbaar tot*
Betrokkene: *geen rechtspersonen*
Verwerkingsverantwoordelijke: *bepaalt doel en middel*
Verwerker: *verwerkt ten behoeve van*


Beginselen
Rechtmatigheid, behoorlijkheid en transparantie
Doelbinding
Minimale gegevensverwerking
Juistheid
Opslagbeperking
Integriteit en vertrouwelijkheid
Accountability verwerkingsverantwoordelijke


Grondslag
Toestemming
Overeenkomst
Wettelijke verplichting
Vitale belangen
Algemeen belang
Gerechtvaardigd belang

12.


Bijzondere persoonsgegevens
Verboden, tenzij:
uitdrukkelijke toestemming
arbeidsrecht / sociaalzekerheidsrecht
vitale belangen
politiek/levensbeschouwelijk/godsdienstig/vakbond
door de betrokkene openbaar gemaakt
rechtsvordering
zwaarwegend algemeen belang
geneeskunde/gezondheidszorg, mits geheimhouder
algemeen belang volksgezondheid
archivering in algemeen belang/onderzoek
Vraag
Is uitdrukkelijke toestemming van de patiënt vereist voor verwerking van medische gegevens in het kader van de behandeling?
Antwoord
Nee, voor verwerking van gegevens in het kader van de behandeling is geen toestemming vereist, mits beroepsbeoefenaar met beroepsgeheim.
(art. 9 lid 2 sub h en lid 3 AVG en art. 30 leden 3 en 4 UAVG)

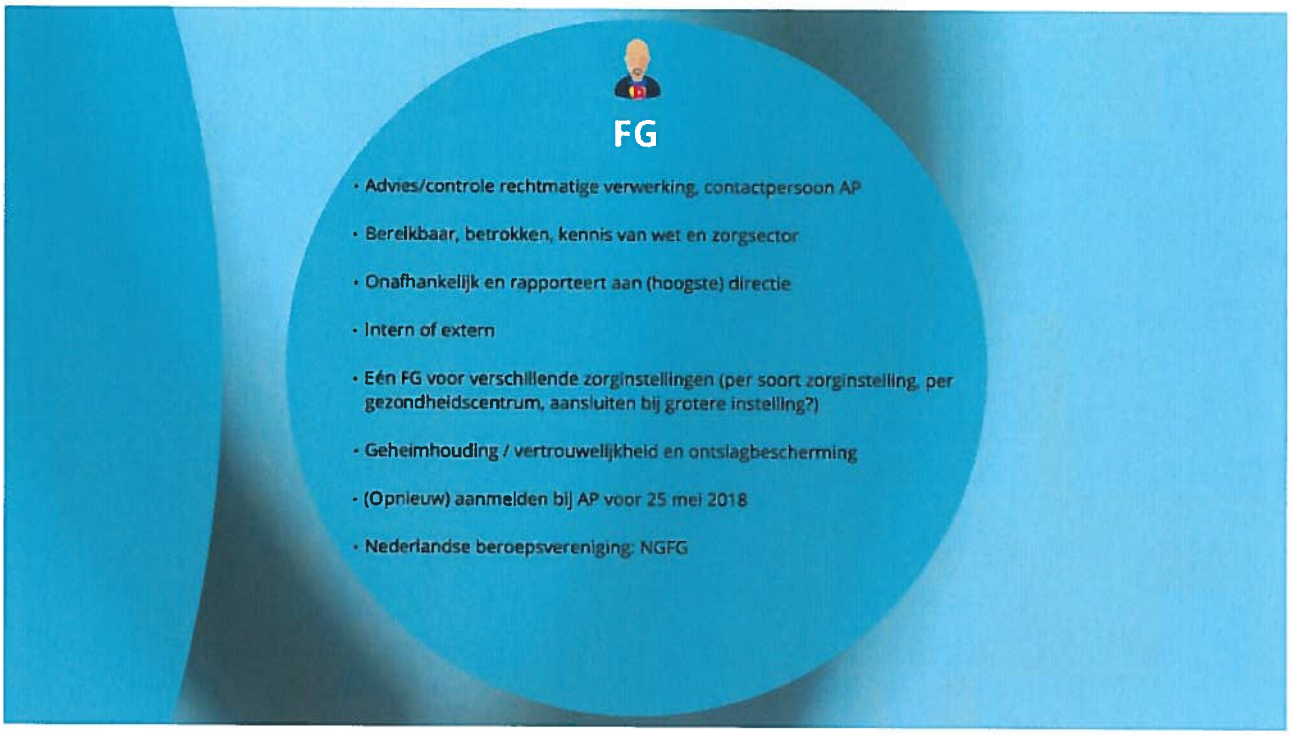
15.

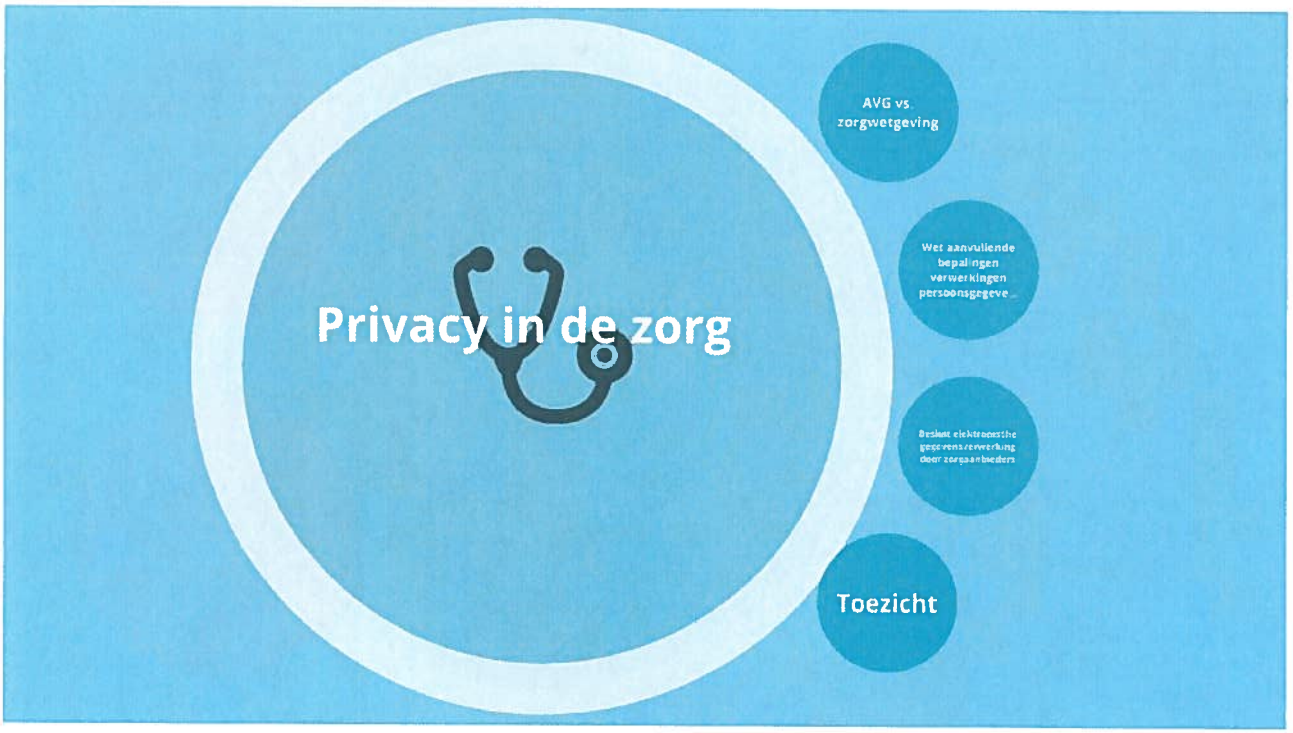

Rechten betrokkene
Recht van inzage
Recht op rectificatie
Recht op gegevenswissing
Recht op beperking van de verwerking
Recht op overdraagbaarheid
Recht van bezwaar
Geen geautomatiseerde individuele besluitvorming

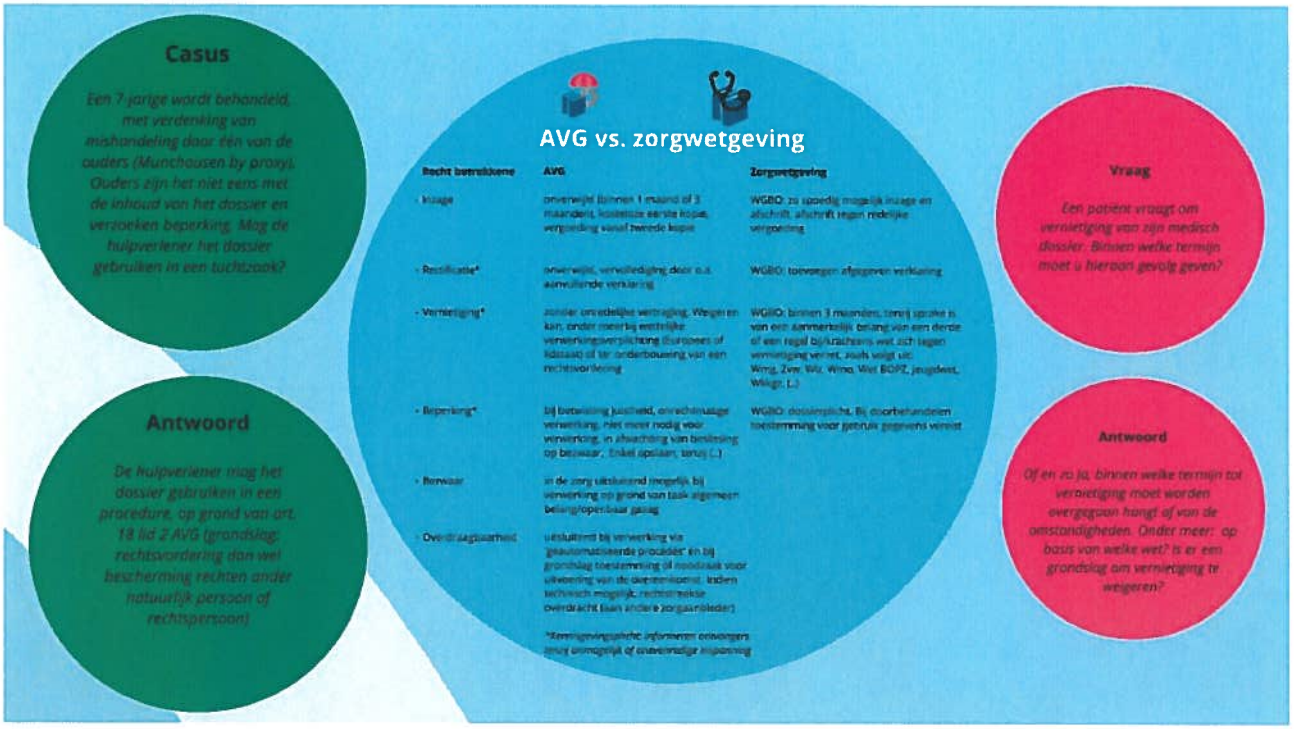
16.


Verplichtingen verwerkingsverantwoordelijke
Informatieplicht
Maatregelen / beveiliging
Privacy by default / privacy by design
DPIA / Gegevensbeschermingseffectbeoordeling
Datalek
Verwerkingsregister
Verwerkersovereenkomst
Functionaris voor de gegevensbescherming
Doorgifte buiten EU
FG
Vraag
Datalek?
a. medische info via Whatsapp aan verkeerde persoon;
b. verlies UZI-pas;
c. DDOS-aanval.
Antwoord
Verstrekken van medische info aan een verkeerde persoon via Whatsapp is een datalek. Bij verlies UZI-pas of DDOS-aanval is niet per definitie sprake van een verlies van gegevens/inbreuk op de beveiliging.

19.


FG
• Advies/controle rechtmatige verwerking, contactpersoon AP
• Bereikbaar, betrokken, kennis van wet en zorgsector
• Onafhankelijk en rapporteert aan (hoogste) directie
• Intern of extern
• Eén FG voor verschillende zorginstellingen (per soort zorginstelling, per gezondheidscentrum, aansluiten bij grotere instelling?)
• Geheimhouding / vertrouwelijkheid en ontslagbescherming
• (Opnieuw) aanmelden bij AP voor 25 mei 2018
• Nederlandse beroepsvereniging: NGFG


Privacy in de zorg
AVG vs. zorgwetgeving
Wet aanvullende bepalingen verwerkingen persoonsgegeve...
Besluit elektronische gegevensverwerking door zorgaanbieders
Toezicht


Casus
Een 7-jarige wordt behandeld, met verdenking van mishandeling door één van de ouders (Munchausen by proxy). Ouders zijn het niet eens met de inhoud van het dossier en verzoeken beperking. Mag de hulpverlener het dossier gebruiken in een tuchtzaak?
AVG vs. zorgwetgeving
Recht betrokkene
AVG
Zorgwetgeving
Vraag
Een patiënt vraagt om vernietiging van zijn medisch dossier. Binnen welke termijn moet u hieraan gevolg geven?
Antwoord
De hulpverlener mag het dossier gebruiken in een procedure, op grond van art. 18 lid 2 AVG (grondslag: rechtsvordering dan wel bescherming rechten ander natuurlijk persoon of rechtspersoon)
Antwoord
Of en zo ja, binnen welke termijn tot vernietiging moet worden overgegaan hangt of van de omstandigheden. Onder meer: op basis van welke wet? Is er een grondslag om vernietiging te weigeren?


Besluit elektronische gegevensverwerking door zorgaanbieders
• Vanaf 1 januari 2018
• FG verplicht voor verantwoordelijke voor elektronisch uitwisselingssysteem en voor zorginstellingen die grootschalig bijzondere persoonsgegevens verwerken. Grijs gebied.
• Vastleggen beleid, procedures, verantwoordelijken rondom elektronisch uitwisselingssysteem en intern zorginformatiesysteem
• NEN-7510: elektronisch uitwisselingssysteem, intern zorginfosysteem
• NEN-7512: veilige verbindingen
• NEN-7513: 'logging' cliëntengegevens
Vraag
Per wanneer moeten zorginstellingen in de zin van de Wkkgz die grootschalig medische gegevens verwerken een FG aanstellen?
Antwoord
Zorginstellingen in de zin van de Wkkgz die grootschalig medische gegevens verwerken, dienen per 1 januari 2018 over een FG te beschikken.

Toezicht

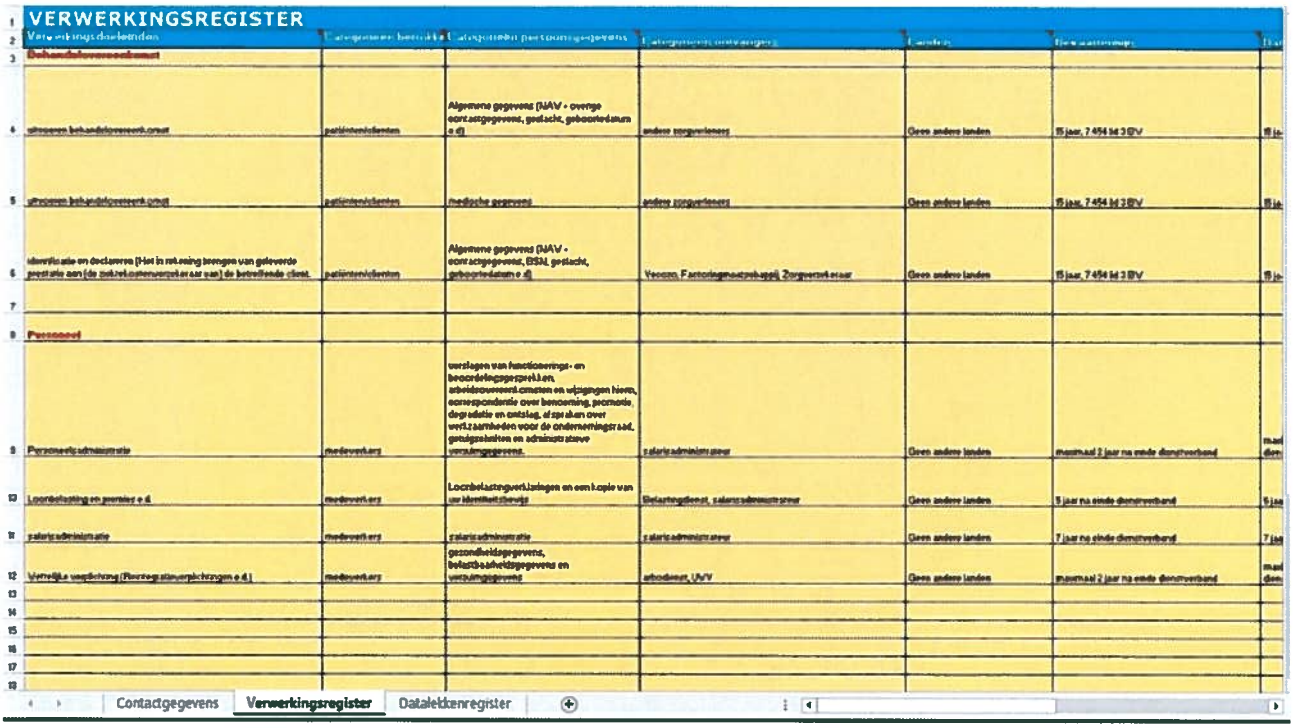
IGJ
- Gezondheidswet
- Wet BIG
- Wlz
- Wmo 2015
- Wkkgz
- Jeugdwet

- *Wetsvoorstel uitbreiding bevoegdheden Inspectie voor de Gezondheidszorg: Geneesmiddelenwet en Wet donorgegevens kunstmatige bevruchting*

NZa
- Wmg

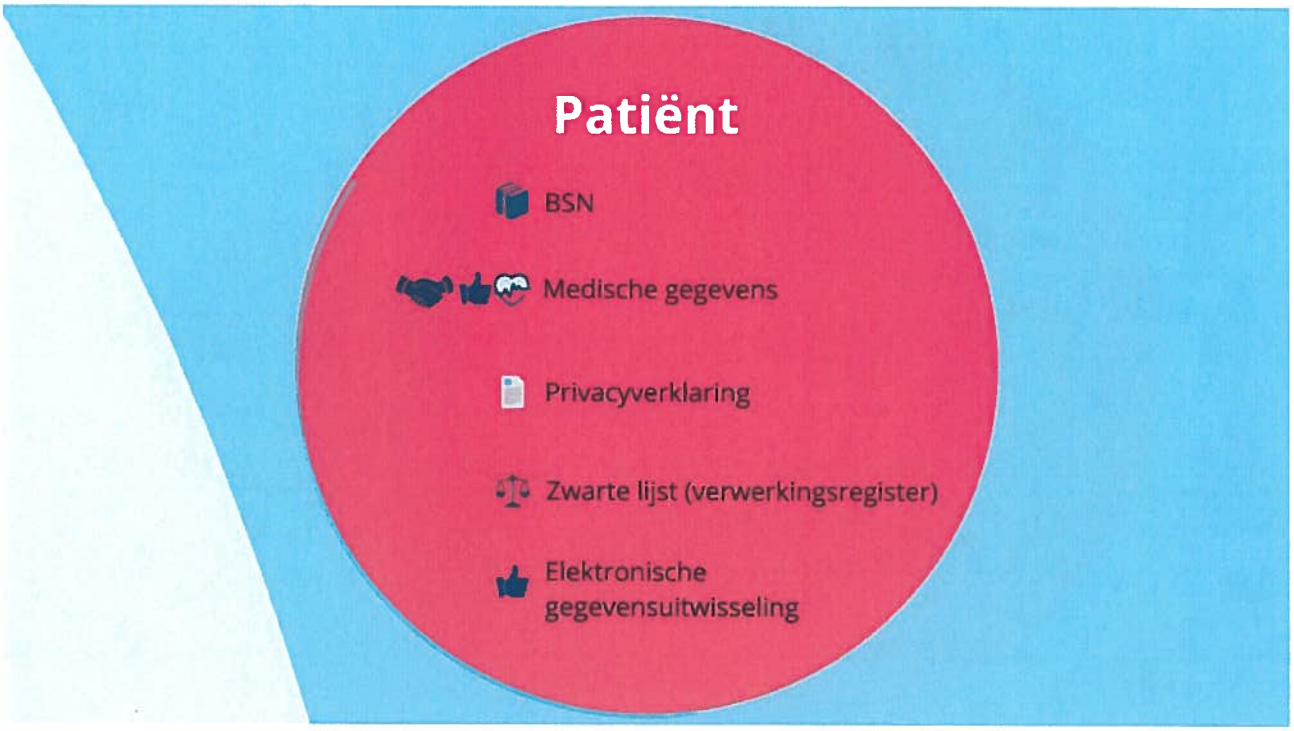
AP
- AVG / verhoogde boetes (10 en 20 mln / 2% en 4%)


Solist vs. zorginstelling
Solistisch werkzame zorgverlener
· Bescherming en beveiliging: ja
· Privacyverklaring: ja
· Verwerkingsregister: ja, want:
1. verwerking is niet incidenteel
2. verwerking van bijz. pg
· Verwerkersovereenkomst: ja
· DPIA: ja, bij waarschijnlijk hoog risico, waaronder:
'besluiten o.b.v. geautomatiseerde verwerking, met rechtsgevolgen voor patiënt'
· FG: nee, want niet grootschalige verw.
Zorginstelling
· Bescherming en beveiliging: ja
· Privacyverklaring: ja
· Verwerkingsregister: ja, want:
1. verwerking is niet incidenteel
2. verwerking van bijz. pg.
· Verwerkersovereenkomst: ja
· DPIA: ja, bij waarschijnlijk hoog risico, waaronder:
1. 'besluiten o.b.v. geautomatiseerde verwerking, met rechtsgevolgen voor patiënt'
2. grootschalige verwerking van bijzondere persoonsgegevens
· FG: ja, mits grootschalige verw.
Verwerkings- en datalekken register

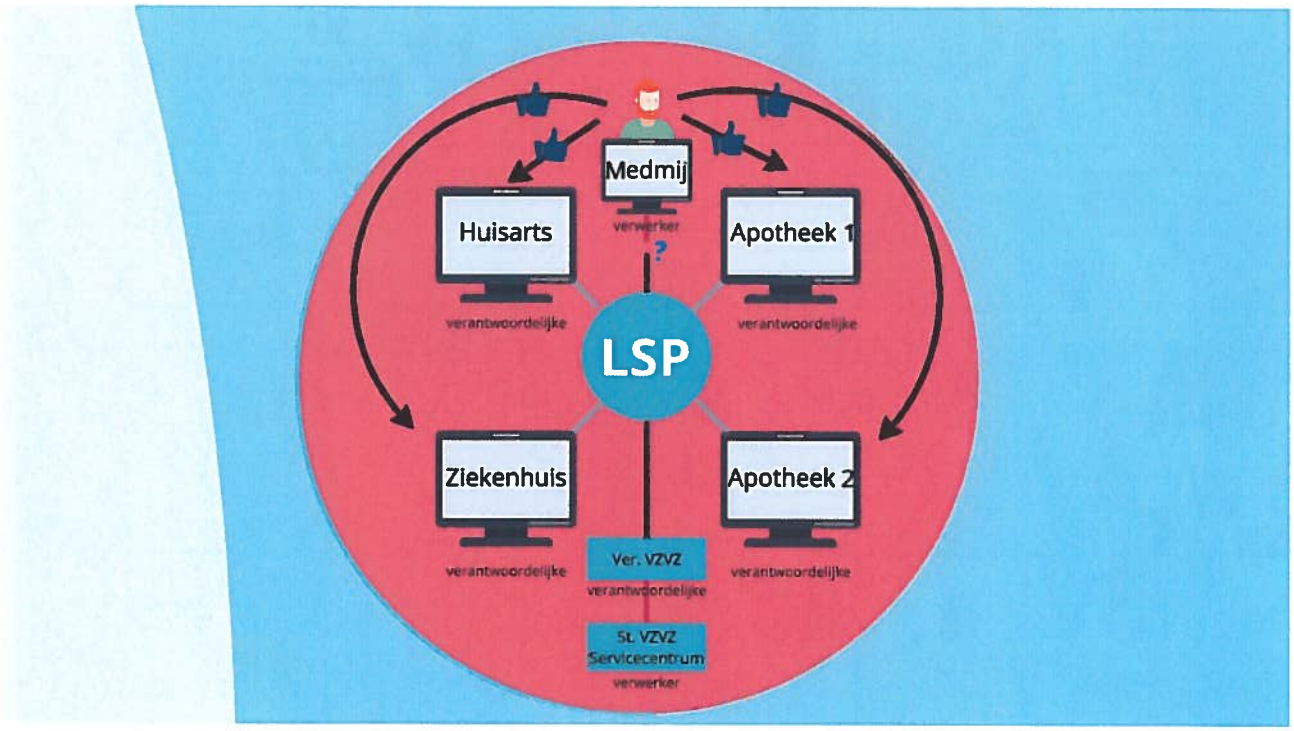

VERWERKINGSREGISTER
Contactgegevens
Verwerkingsregister
Datalekkenregister

	DATALEKKENREGISTER							
2	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
3	laptop met medisch dossier achtergelaten in de trein	nog niet bekend	30-3-2018	30-3-2018	nee	NAW, contactgegevens, medische gegevens client	client	
4	idem	idem	idem	idem	idem	idem	idem	idem
5	medische gegevens verzonden via (onbeveiligde) e-ma	nog niet bekend	5-4-2018	7-4-2018	nee	NAW, contactgegevens, medische gegevens client	client	
6	wachtwoord tot database met medische dossiers laten s	onduidelijk	niet bekend	9-4-2018	nee	NAW, contactgegevens, medische gegevens client	client	onbekend,
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								

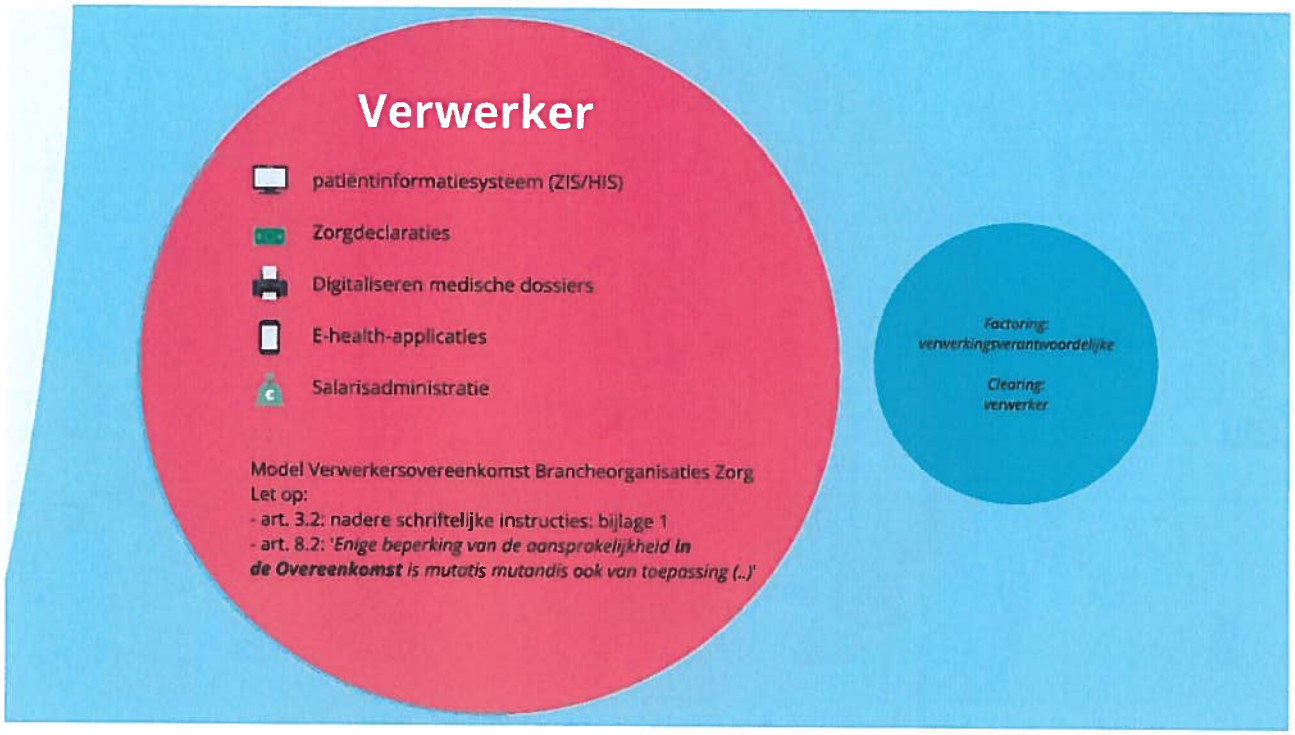
Contactgegevens | Verwerkingsregister | **Datalekkenregister**

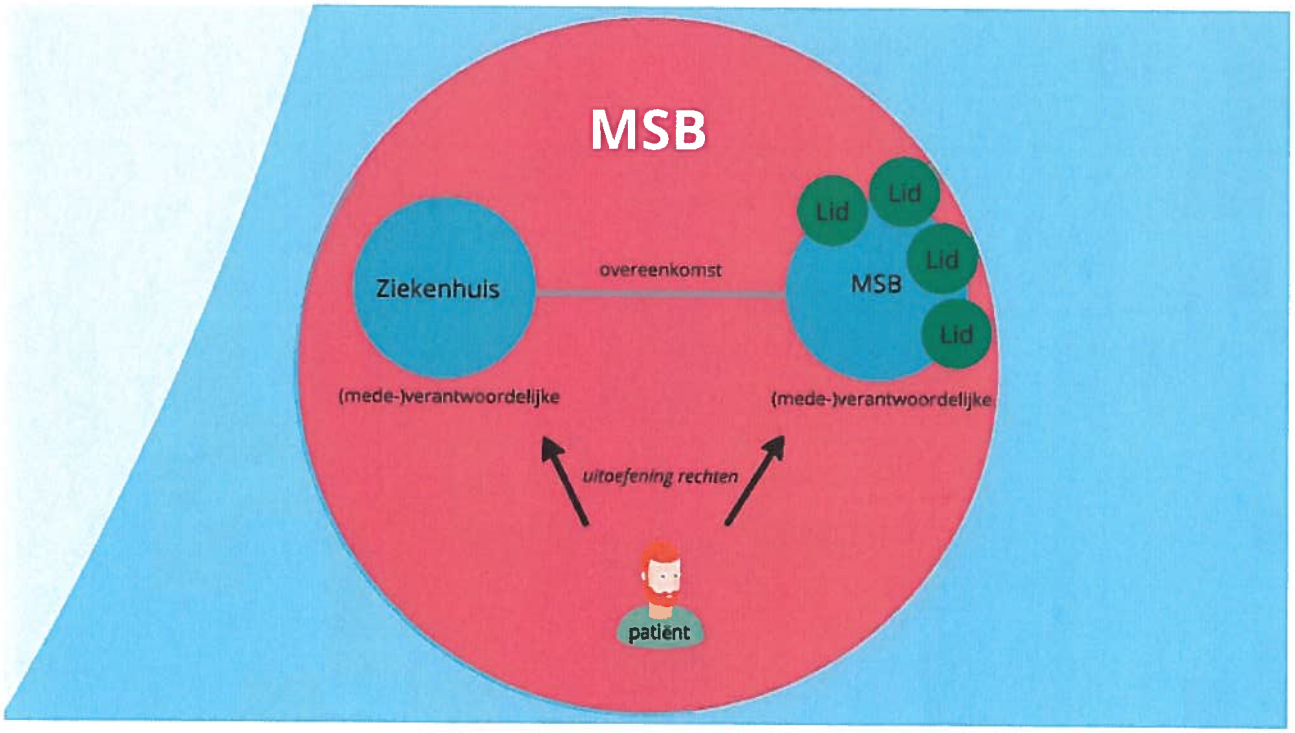

Patiënt
BSN
Medische gegevens
Privacyverklaring
Zwarte lijst (verwerkingsregister)
Elektronische gegevensuitwisseling

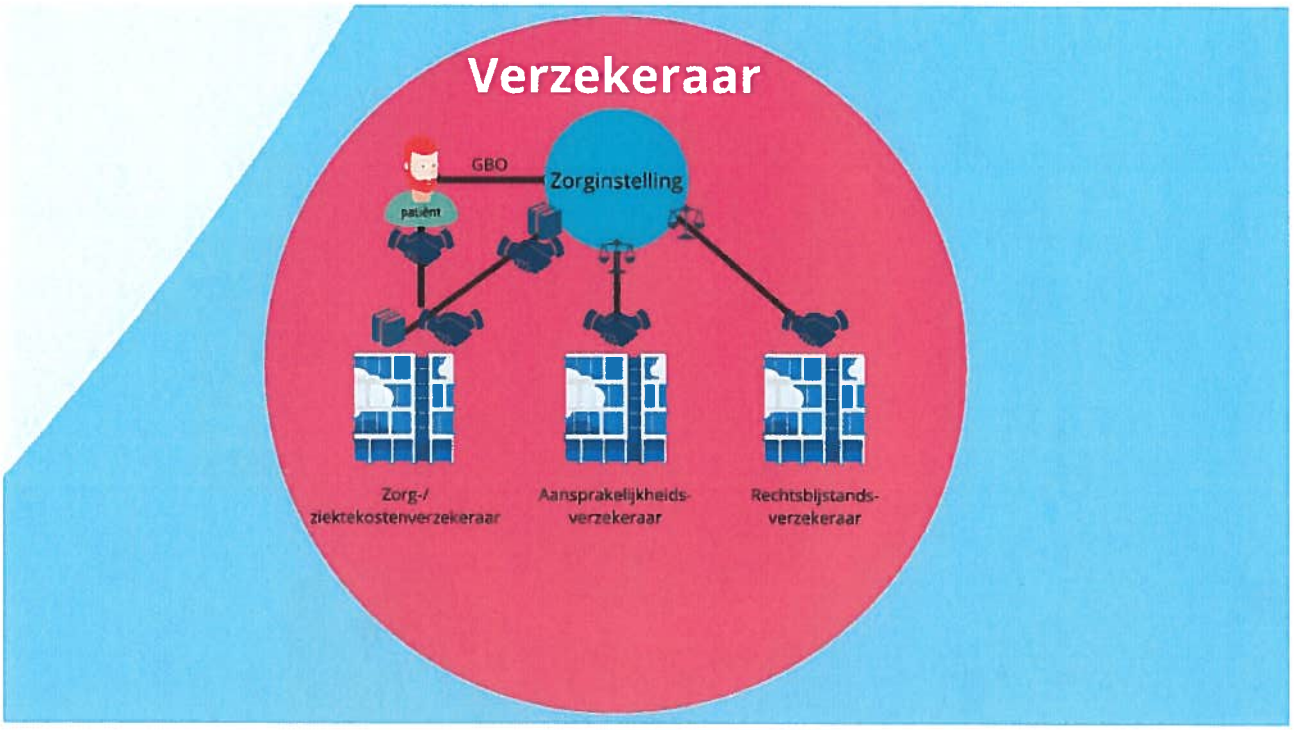
35.


Medmij
verwerker
Huisarts
verantwoordelijke
Apotheek 1
verantwoordelijke
LSP
Ziekenhuis
verantwoordelijke
Apotheek 2
verantwoordelijke
Ver. VZVZ
verantwoordelijke
St. VZVZ Servicecentrum
verwerker

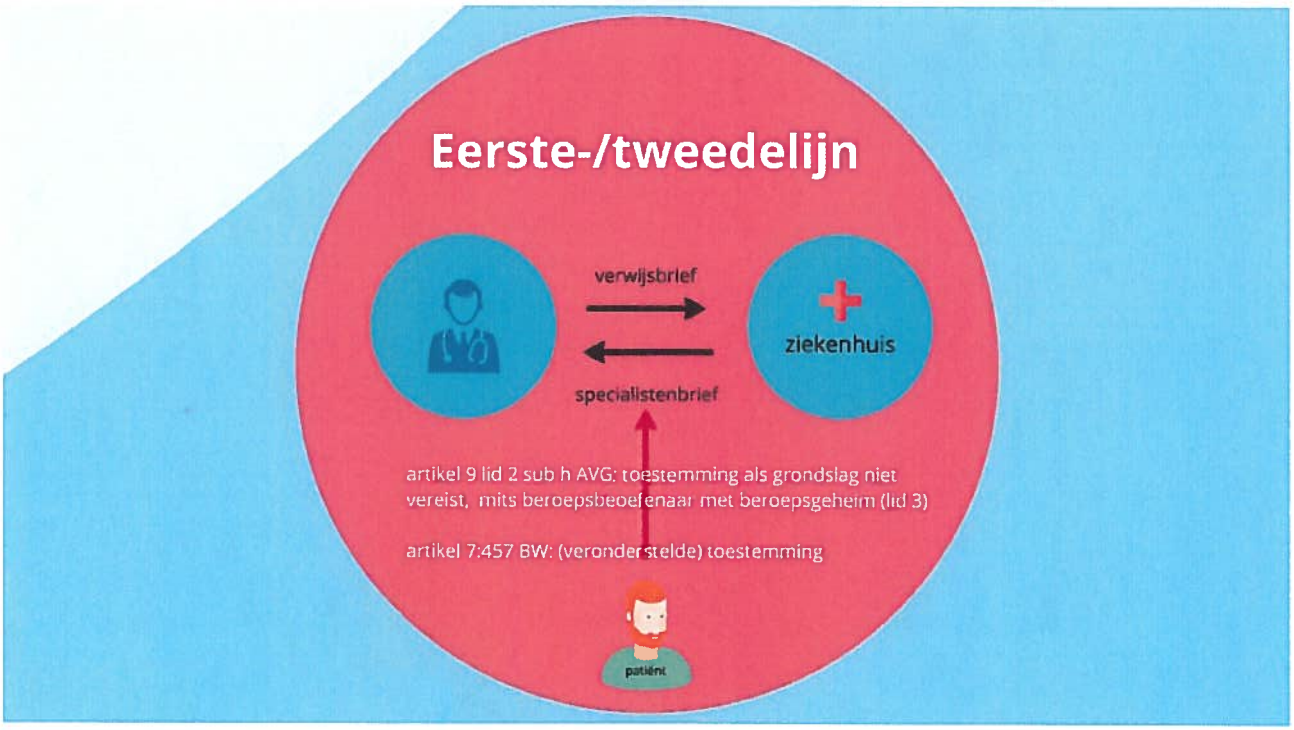
36.


Verwerker
patiëntinformatiesysteem (ZIS/HIS)
Zorgdeclaraties
Digitaliseren medische dossiers
E-health-applicaties
Salarisadministratie
Model Verwerkersovereenkomst Brancheorganisaties Zorg
Let op:
- art. 3.2: nadere schriftelijke instructies: bijlage 1
- art. 8.2: 'Enige beperking van de aansprakelijkheid in de Overeenkomst is mutatis mutandis ook van toepassing (..)'
Factoring:
verwerkingsverantwoordelijke
Clearing:
verwerker

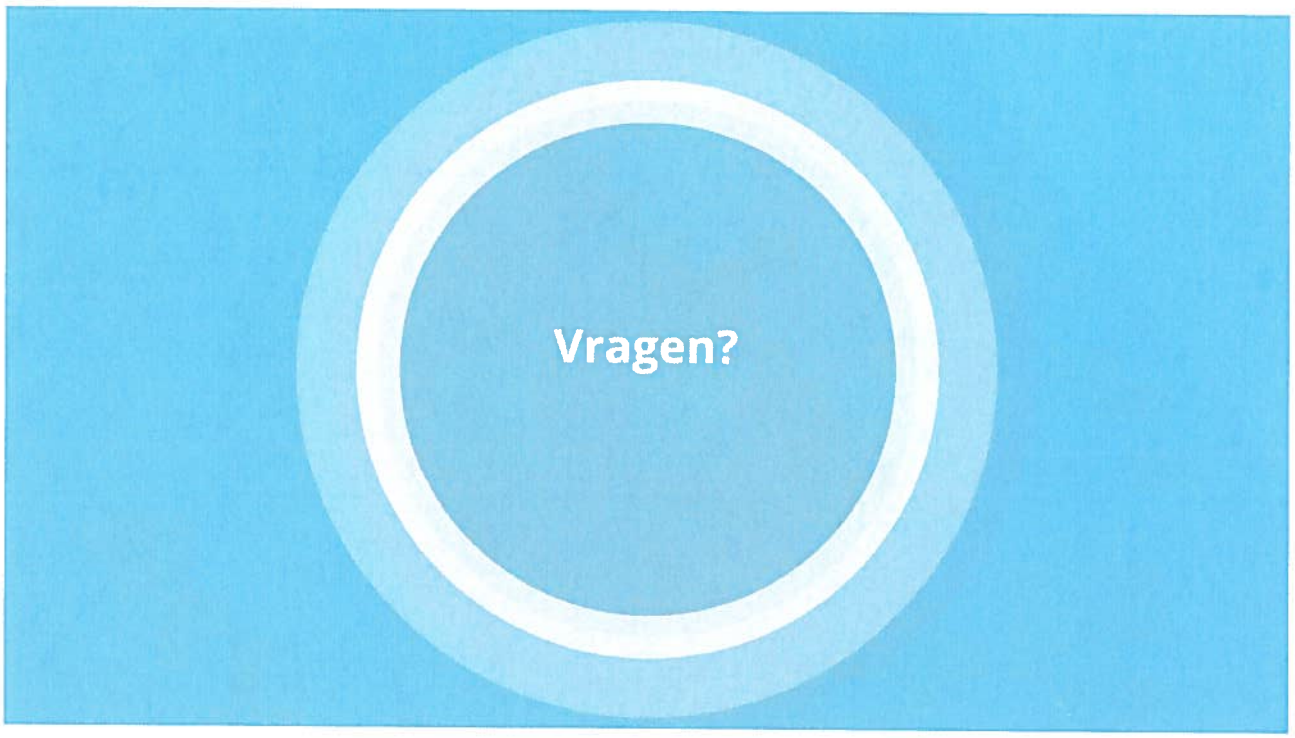

MSB
Ziekenhuis
overeenkomst
MSB
Lid
Lid
Lid
Lid
(mede-)verantwoordelijke
(mede-)verantwoordelijke
uitoefening rechten
patiënt


Verzekeraar
GBO
Zorginstelling
patiënt
Zorg-/
ziektekostenverzekeraar
Aansprakelijkheids-
verzekeraar
Rechtsbijstands-
verzekeraar

39.


Eerste-/tweedelijn
verwijsbrief
specialistenbrief
ziekenhuis
artikel 9 lid 2 sub h AVG: toestemming als grondslag niet vereist, mits beroepsbeoefenaar met beroepsgeheim (lid 3)
artikel 7:457 BW: (veronderstelde) toestemming
patiënt

40.


Vragen?