Wat is DIZRA?

DIZRA staat voor de referentiearchitectuur van een duurzaam informatiestelsel in de zorg. Het bestaat uit uitgangspunten, instrumenten, kennisthema's en praktische richtlijnen.

De zorg bouwt aan een duurzaam informatiestelsel. Een stelsel waarin data en services digitaal vindbaar, toegankelijk, uitwisselbaar en herbruikbaar zijn. DIZRA is de referentiearchitectuur voor dit informatiestelsel in de zorg. Het is een product van IT-Architecten voor IT-Architecten. Met DIZRA borgen we de samenhang en de duurzaamheid van het informatiestelsel, we delen kennis en verhogen de kwaliteit van de afspraken.

Dit doen we door het beschrijven van:

1. Een **manifest** met uitgangspunten. Het manifest beschrijft de uitgangspunten voor het maken van architectuurkeuzes. Met dezelfde uitgangspunten verkrijgen we meer samenhang.
2. Een **begrippenlijst** om de terminologie te verklaren en te definiëren**.** Met de begrippen werken we aan een gemeenschappelijk taalgebruik zodat we elkaar beter begrijpen.
3. De uitgangspunten zijn uitgewerkt in **thema's.** In een thema is de motivatie en de rationale van een uitgangspunt beschreven**.**
4. Meer samenhang ontstaat door het raamwerk met **rollen.** De rollen geven structuur aan de afspraken en stimuleert hergebruik van afspraken. Voor iedere rol wordt beschreven wat haar verantwoordelijkheden zijn. Aan de hand van deze verantwoordelijkheden zijn de **richtlijnen** opgesteld. De richtlijnen zijn de implicaties van de gehanteerde uitgangspunten..

DIZRA is in opdracht van het Informatieberaad Zorg ontwikkeld. Het informatiestelsel is nodig om de zorg nog beter, betaalbaarder en toegankelijker te maken. Als IT-Architecten in de zorg dragen we bij door het stelsel uitgangspunten, structuur en samenhang te geven. DIZRA is het gezamenlijke resultaat van alle gesprekken en de ingebrachte kennis, kunde en ervaring van IT-Architecten in de zorg. DIZRA is vakinhoudelijk en vereist daarom kennis van informatievoorziening en informatietechnologie.

> **Status van DIZRA als referentiearchitectuur voor het informatiestelsel in de zorg:**
>
> Het Informatieberaad Zorg heeft de volgende besluiten genomen:
>
> - 12-2018: De principes zijn vastgesteld
> - 09-2019: De richtlijnen zijn vastgesteld onder voorwaarde van beproeving
> - 04-2020: De resultaten van de beproeving zijn teruggemeld aan het informatieberaad. Het informatieberaad heeft op basis hiervan besloten DIZRA vast te stellen.

Van start gaan gaan is de beste manier om de referentiearchitectuur te leren kennen. Je kunt het hoofdstuk van start gaan gebruiken als leeswijzer voor het beginnen met DIZRA.

Normenkader downloaden

Het normenkader kan gedownload worden als Excel-bestand. Klik hieronder om het bestand te downloaden.

Normenkader Normenkader V2020-03.xlsx - 12KB

Reactie geven

De ontwikkeling van DIZRA is een continu én dynamisch proces. We nodigen iedereen uit om een reactie te geven en jouw vragen, opmerkingen en ervaringen te delen. Alleen dan komen we tot een referentiearchitectuur die ons allen helpt in de realisatie van een duurzaam informatiestelsel in de zorg.

Reacties die we graag ontvangen gaan bijvoorbeeld over:

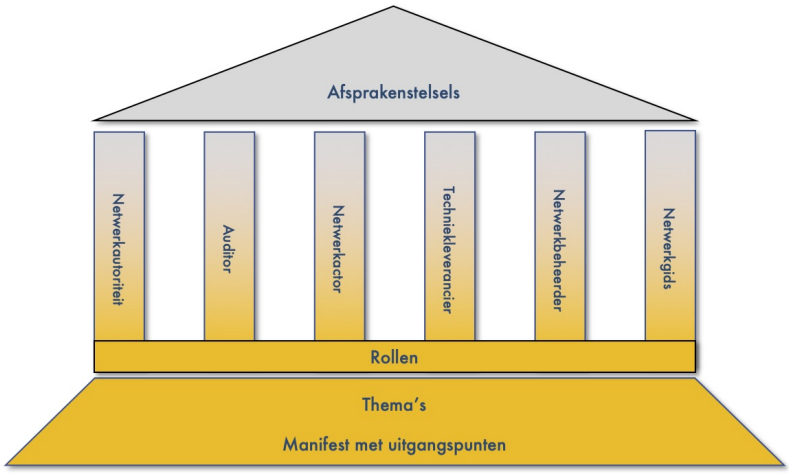
- verdere verduidelijking van een onderdeel;
- actualisering door nieuwe inzichten of veranderende omgeving;
- toevoegingen;
- voorbeelden hoe een onderdeel van DIZRA in de praktijk toegepast kan worden;
- vragen of twijfels hoe je iets moet uitleggen of toepassen.

Je kunt reageren door een mail te sturen naar: architectuurcommunityzorg@zinl.nl

Van start gaan

Start met het gebruiken van de principes, de instrumenten en neem kennis van de thema's met de richtlijnen.Met DIZRA maak je een snelle start.

DIZRA is een referentiearchitectuur. Maar wat betekent dat? Kort gezegd kun je zeggen dat het een fundament is waarop anderen kunnen voortbouwen. Een gemeenschappelijke basis dus. Omdat we vanuit een zelfde basis vertrekken ontstaat er samenhang.



Figuur 1: Samenhang door een gemeenschappelijke basis

DIZRA heeft uitleg nodig om de uitgangspunten en de structuur te begrijpen. We moeten hiervoor met elkaar in gesprek gaan. In dit hoofdstuk beschrijven we hoe Amber in gesprek gaat met Ben en uitleg geeft over DIZRA. We zullen ze opnieuw tegenkomen bij de uitleg over de rollen in DIZRA. Met DIZRA gaan we je op weg helpen met het maken van afspraken. DIZRA hoopt je reisgenoot te zijn naar de bestemming van je afspraken.

> DIZRA wil je op weg helpen met het maken van afspraken. We beschrijven hoe Amber in gesprek gaat met Ben over de afspraken. Ben is programmamanager en Amber IT-Architect. We introduceren ze in dit hoofdstuk. In de beschrijving van de rollen zul je ze weer tegenkomen in hun gesprek over DIZRA en de afspraken die nodig zijn voor vertrouwen, vindbaarheid, toegankelijkheid, interoperabiliteit en hergebruik van data.

Manifest en thema's

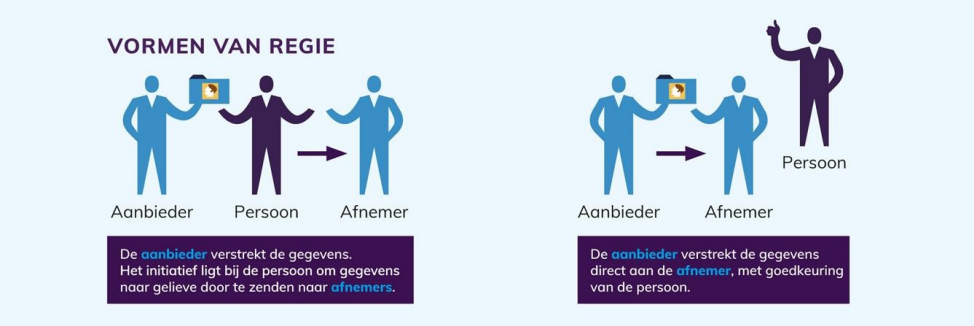
Ben is programmamanager voor het realiseren van afspraken. Afspraken om berichtjes uit te wisselen zoals hij het zelf noemt. Wat moet ik met het manifest vraagt hij aan Amber. Amber is IT-Architect van het programma. Het manifest bevat de principes, oftewel de uitgangspunten voor een duurzaam informatiestelsel in de zorg. Het zijn de principes voor de architectuur van het informatiestelsel.

Het Informatieberaad Zorg heeft de principes vastgesteld vertelt Amber. We zijn niet het enige programma dat afspraken maakt. We realiseren samenhang tussen de afspraken omdat we dezelfde uitgangspunten hanteren.

Een aantal van de principes is uitgewerkt in een thema. Daarnaast is het thema vertrouwensinfrastructuur opgenomen. In dit thema wordt beschreven welke afspraken nodig zijn om vertrouwen te verkrijgen tussen de deelnemers van een netwerk.

Regie op gegevens

Een van de principes van DIZRA is regie op eigen gezondheidsdata. Ik noem het, zegt Amber, omdat de vormen van regie richtinggevend zijn voor de richtlijnen. In onderstaand figuur zijn de twee vormen van regie weergegeven.



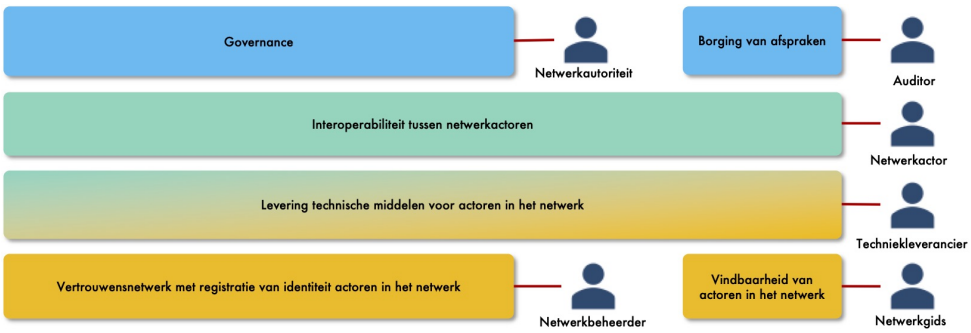
Figuur 1: Regie op gegevens (bron: Programma regie op gegevens)

Regie op gegevens is van toepassing in alle sectoren waarin persoonsgegevens een rol spelen. Banken en telecombedrijven ontwikkelen bijvoorbeeld toepassingen voor hun klanten om regie op gegevens te verkrijgen. Voor de zorg kunnen we hergebruik maken van deze toepassingen. Graag zegt Ben. Anders krijgen we weer de situatie dat iedereen zijn eigen toepassing heeft. Staat mijn telefoon weer vol. Mensen willen inderdaad toepassingen waarmee ze bijvoorbeeld zowel bij hun bank als bij hun huisarts toestemming kunnen geven gaat Amber verder. Dat kunnen we bereiken door gebruik te maken van dezelfde standaarden. Dat is kostenefficiënt.

DIZRA houdt rekening met de vormen van regie op gegevens. In het raamwerk zijn de rollen opgenomen waarmee we beide vormen ondersteunen zegt Amber.

Het raamwerk

Ben kijkt naar het plaatje met de rollen en de functies. Dat is best een ingewikkeld plaatje mompelt hij. Moet ik dat allemaal gaan regelen vraagt hij aan Amber. Kan het niet eenvoudiger? In het raamwerk zijn de rollen opgenomen begint Amber. Voor iedere rol moeten afspraken gemaakt worden. In het onderstaande plaatje staat kort wat iedere rol doet.



Figuur 2: Raamwerk van afspraken

Nou kom maar op zegt Ben. Het is inderdaad een heel verhaal vervolgt Amber. Het geheel moet werken als één systeem, een ecosysteem. Dat maakt het complex. Zeer zeker als je niet bekend bent met een afsprakenstelsel en met informatietechnologie. Het is ook heel abstract. Waarom is dat vraagt Ben. Kan het niet concreter? De toepassingen zijn concreet zegt Amber, maar het model is abstract. Je kunt het model op vele manieren toepassen. Dat is nodig omdat de zorg vele toepassingen kent.

Ik za het model uitleggen op basis van de rollen. Ik zal ingaan op iedere rol en wat het betekent. Maar ook over de afspraken die we moeten maken voor die rol. Voor de afspraken is het het noodzakelijk dat we weten welke partij welke rol gaat spelen. Op ieder van de onderwerpen die we behandelen zijn

boekenkasten vol geschreven. De uitleg die ik geef is daarom globaal zegt Amber. We hebt dus specialisten nodig om de afspraken te maken zegt Ben. Klopt zegt Amber.

De uitleg van Amber is te lezen in de sectie rollen.

Manifest

Het manifest beschrijft de principes voor het informatiestelsel in de zorg.

We werken samen aan een duurzaam informatiestelsel. Dit is een stelsel waarin we afspraken maken over regie en hergebruik van data zodat de zorg doeltreffender en doelmatiger is. Door middel van principes maken we onze uitgangspunten bekend.

1. In het informatiestelsel hebben burgers **regie op hun eigen gezondheidsdata** en kunnen deze data meenemen en delen in hun reis door het zorglandschap en in het netwerk van zorgverleners en ondersteuners dat zich rondom hen vormt.
2. In het informatiestelsel **spreken we een gemeenschappelijke taal** en hanteren gemeenschappelijke terminologie, waarbij we de contextuele verschillen omarmen.
3. De **data** blijft **bij de bron**, onder de verantwoordelijkheid van de bronhouder, voor een veilig en vertrouwd informatiestelsel waarin het voor burgers transparant is welke bronhouders welke gezondheidsgegevens registreren en wie het raadpleegt.
4. Het informatiestelsel hanteert een **gelijk speelveld voor alle leveranciers**. Afspraken worden gemaakt over het gebruik van standaarden, niet over het gebruik van een product of dienst. Iedere organisatie kiest haar eigen leveranciers voor het implementeren van de standaarden.
5. Het informatiestelsel is **duurzaam** doordat het relevant is en blijft. Het omarmt voor nu en in de toekomst de complexiteit van meerdere standaarden in een stelsel waarin verandering en innovatie welkom is.
6. Data wordt enkelvoudig geregistreerd bij de bron en vervolgens beschikbaar gesteld voor meervoudig gebruik in verschillende toepassingen. Hiervoor hanteert het informatiestelsel de **FAIR-data** principes.
7. Data is **machineleesbaar**, machines begrijpen de data, zonder daarbij de leesbaarheid van deze data voor mensen uit het oog te verliezen. Dit opent de mogelijkheden van data-analyse en data-science.
8. In het informatiestelsel wordt **federatief** samengewerkt aan afspraken voor data en voor diensten. Iedereen implementeert deze afspraken en is aanspreekbaar op het nakomen van de afspraken en de kwaliteit van de implementatie.
9. Semantische en technische interoperabiliteit wordt in het informatiestelsel gerealiseerd door te kiezen voor **open internationale standaarden**. Iedere deelnemer aan het stelsel moet voldoen aan de standaarden die zijn afgesproken.

Bovenstaande uitgangspunten worden gehanteerd naast de vigerende wet- en regelgeving waaraan iedere rechtspersoon moet voldoen. Wet- en regelgeving zoals gegevensbescherming door ontwerp en standaardinstellingen. Wet- en regelgeving is dus niet als principe opgenomen. De uitgangspunten zijn in de thema's en de richtlijnen verder uitgewerkt en gemotiveerd.

Herkomst principes

In dit hoofdstuk verwijzen we vanuit de oorspronkelijke principes naar de uitgangspunten in het manifest. DIZRA hanteert het manifest met uitgangspunten.

In het manifest worden de uitgangspunten kort en bondig weergegeven. In onderstaande tabellen is de vertaling van principe naar manifest weergegeven.

Basisprincipes

Van basisprincipe naar afgeleid principe.

Basisprincipe	Afgeleid principe
BP1 Mensgericht: "*bij het verstrekken van gegevens over mij, aan mij, houden dienstverleners rekening met mijn wensen en kunnen.*".	AP1, AP2, AP6, AP8
BP2 Organisatie rondom de mens: "*dienstverleners uit verschillende organisaties delen gegevens over mijn gezondheid, om gezamenlijk toe te werken naar de gewenste uitkomsten van mijn zorg en ondersteuning*".	AP2, AP11, AP14, AP16, AP19, AP21
BP3 Regie op gezondheid: "*Ik kan regie nemen op de gegevens over mijn gezondheid*".	AP11, AP12, AP15
BP4 Vertrouwen: "*ik kan er op vertrouwen dat mijn gegevens de juiste zorg krijgen*".	AP3, AP7, AP8, AP9, AP10. AP12, AP13, AP17, AP18
BP5 Verantwoordelijk: "*ik weet wie verantwoordelijk is voor de verwerking van mijn gegevens en weet wie ik kan aanspreken*".	AP4, AP5, AP8, AP9, AP10, AP19
BP6 Vindbaar en toegankelijk: "*mijn gegevens zijn eenvoudig te vinden en te hergebruiken.*"	AP6, AP11, AP14, AP15, AP16, AP19, AP20

Afgeleide principes

Van afgeleid principe naar manifest.

Afgeleid principe	Manifest	Korte titel
AP1 Vanuit een gebruiksdoel: "*onze bouwstenen zijn ontwikkeld vanuit de eindgebruikers van het informatiestelsel en zijn of haar gebruiksdoelen*".	MP5	Duurzaam
AP2 Bruikbaar en gebruiksvriendelijk: "*onze gegevensdiensten zijn bruikbaar en gebruiksvriendelijk, en dragen bij aan een goede gebruikservaring*".	MP5	Duurzaam
AP3 Een gemodereerd ecosysteem: "*we voldoen aan de gemeenschappelijke afspraken om mee te doen aan het informatiestelsel*".	MP4	Gelijk speelveld
AP4 Federatief: "*we ontwikkelen en beheren het informatiestelsel gezamenlijk*".	MP8	Federatief

AP5 Eenduidige verantwoordelijkheid: "*we hanteren een heldere en eenduidige verantwoordelijkheid en zijn daarop aanspreekbaar*"	MP8	Federatief
AP6 Gestandaardiseerde diversiteit: "*we accepteren contextuele diversiteit, maar streven naar standaardisatie*".	MP5	Duurzaam
AP7 Verantwoord gebruik: "*we dragen zorg voor de bescherming van persoonsgegevens*".	MP3	Data bij de bron
AP8 Transparantie in kwaliteit: "*we zijn transparant over de kwaliteit van onze gegevens en gegevensdiensten"*.	MP8	Federatief
AP9 Open voor innovatie en verbetering: "*we erkennen dat we lerende zijn en continu moeten werken aan verbetering*".	MP5	Duurzaam
AP10 Decentraal: "*we houden gegevens decentraal en maken deze toegankelijk bij de bron*".	MP3	Data bij de bron
AP11 Herbruikbare gegevens: "*onze gegevens worden eenmalig geregistreerd en we borgen herbruikbaarheid voor meervoudig gebruik*".	MP6	FAIR-data
AP12 Regie over gegevens: "*we stellen patiënten, cliënten en burgers in staat om controle en regie te nemen over hun gegevens*"	MP1	Regie op gegevens
AP13 Open waar het kan, besloten waar het moet: "*onze gegevens zijn open waar het kan en besloten, geauthenticeerd en geautoriseerd, waar het moet*".	MP6	FAIR-data
AP14 Een gemeenschappelijk vocabulaire: "*onze gegevens zijn uitwisselbaar met een gemeenschappelijk vocabulaire zodat we elkaar kunnen begrijpen*".	MP2	Gemeenschappelijke taal
AP15 Machineleesbaar als fundament: "*onze gegevens zijn primair leesbaar voor machines, secundair voor mensen*".	MP7	Machineleesbaar
AP16 Een persoonlijk netwerk voor gezondheid: "*we organiseren gegevens in een netwerk voor persoonlijke gezondheid*".	MP1	Regie op gegevens
AP17 Zo weinig mogelijk, zo veel als nodig: "*we minimaliseren de hoeveelheid gegevens die we registreren en uitwisselen, zowel vanuit gegevensbescherming als vanuit efficiency en effectiviteit*".	MP3	Data bij de bron
AP18 Respectvol omgaan met gegevens: "*we onderkennen dat gegevens waarde vertegenwoordigen en handelen daarnaar*".	MP3	Data bij de bron
AP19 Beschikbaar en vindbaar: "*we zorgen ervoor dat gegevensdiensten altijd en overal beschikbaar en vindbaar zijn*"	MP6	FAIR-data
AP20 Taal los van transport: "*we maken onderscheid tussen taal en transport en koppelen dat los van elkaar*".	MP5	Duurzaam
AP21 Internationale standaarden: "*we maken gebruik van open standaarden, internationaal boven nationaal*".	MP9	Open internationale standaarden

Begrippenlijst

De begrippen zoals deze in de referentiearchitectuur worden gehanteerd.

Aansluiting

Bedrijfsfunctie voor het overeenkomen van deelname aan een netwerk. Door de aansluiting wordt een rechtspersoon deelnemer aan het netwerk.

Aansluitovereenkomst

Zie deelnemersovereenkomst.

Aansluitvoorwaarden

Voorwaarden waaraan een rechtspersoon moet voldoen om aangesloten te mogen worden op het vertrouwde netwerk voor gegevensuitwisseling. De aansluitvoorwaarden zijn onderdeel van het stelsel van afspraken voor netwerken.

Actor

Een actor is een rol in de context van een interactie met een systeem. De actor specificeert een rol die gespeeld wordt door een rechtspersoon, een natuurlijk persoon, een systeem of een machine. De rollen die gespeeld kunnen worden zijn een classificatie van gedrag.

Afsprakenstelsel

Een afsprakenstelsel is een governance raamwerk met afspraken voor het realiseren van vertrouwen. Afspraken kunnen als wettelijke norm zijn vastgelegd of als juridische overeenkomst.

Architectuur

Een beschrijving van een complex geheel, en van de principes die van toepassing zijn op de ontwikkeling van het geheel en zijn onderdelen.

Attest

Een attest is een elektronisch bewijs, een (officiële) verklaring die een mondelinge bewering versterkt, ondersteunt, wettigt. DIZRA gebruikt het woord voor de data die elektronisch ondertekend wordt door een netwerkactor. De netwerkactor geeft daarmee een getuigschrift af dat een bewering waar is.

Bron: Wikipedia met aanvulling

Auteur

De auteur is de producent van data.

Authenticatie

Een elektronisch proces. Met de authenticatie wordt bevestiging verkregen van identificerende kenmerken van een natuurlijke persoon of rechtspersoon.

Authenticatiemiddel

Een middel waarmee de authenticatie van een rechtspersoon of natuurlijk persoon kan worden uitgevoerd.

Autorisatie

Het verlenen van de bevoegdheid tot het uitvoeren van een dienst aan een geauthenticeerd persoon. Autorisatie is GEEN synoniem voor machtiging.

Betrokkene

Een natuurlijk persoon waarvoor persoonsgegevens worden verwerkt.

Brondossierhouder

Zie bronhouder.

Bronhouder

Een bronhouder is een rechtspersoon die data vindbaar en toegankelijk maakt.

Conceptueel model

Een model van concepten. Ieder concept wordt als onderwerp beschreven in objecten. Het conceptueel model vormt de ontologie voor het onderwerp. Een gangbare vorm voor het beschrijven van concepten is: onderwerp - predicaat - object. Een UML klassendiagram kan gebruikt worden voor de visualisatie.

Deelnemer

Deelnemer aan een netwerk. Een persoon moet zich aansluiten bij een netwerk om deelnemer te zijn.

Dienst

Een afgebakende prestatie van een rechtspersoon (de dienstverlener), die voorziet in een behoefte van haar omgeving (de afnemers).

DIZRA

Duurzaam Informatiestelsel in de Zorg Referentie Architectuur; zie Referentiearchitectuur

Domein

Het werkingsgebied waarin een element (principe, dienst, standaard, ...) wordt of kan worden toegepast.

Domeinmodel

Een conceptueel overzicht van een domein waarin de elementen zijn geïdentificeerd die in het domein van belang zijn.

Ecosysteem

Een ecosysteem is normaal gesproken een geheel van planten en dieren (bron: Van Dale). Voor het informatiestelsel wordt het ecosysteem gezien als het systeem dat met het geheel van afspraken wordt gerealiseerd.

Elektronisch identificatiemiddel

Een middel waarmee een persoon kan worden geïdentificeerd. Het middel moet het identificerende kenmerk bevatten.

Elektronische identificatie

Het proces van identificeren van een persoon.

Federatie

Een afsprakenstelsel maakt afspraken over een federatief stelsel van diensten. De term federatie wordt gebruikt om aan te geven dat iedere deelnemer in het netwerk autonoom is en zelf verantwoordelijk is voor de implementatie en het operationeel houden van diensten.

Federatief netwerk

Synoniem voor netwerk van autonome deelnemers. Zie ook federatie.

Federatief stelsel

Het afsprakenstelsel is een federatief stelsel. Zie ook federatie.

Gegevensafnemer

De gegevensafnemer verwerkt data afkomstig van een bronhouder.

Gegevensproducent

Zie auteur.

Gids naar gegevensbronnen

Een gids naar gegevensbronnen is een rol van een dienstverlener die verantwoordelijk is voor het realiseren van een adresboek van gegevensbronnen.

Gids naar gezondheidsgegevens

Een gids naar gezondheidsgegevens is een specialistische rol van een bronhouder. Het bevat gezondheidsgegevens over een persoon in de vorm van verwijzingen naar bronhouders die gegevens hebben geregistreerd over die persoon.

Governance autoriteit

Een rol voor het uitvoeren van de governance op een raamwerk van afspraken.

Grondslag voor de verwerking

Een van de 6 grondslagen zoals genoemd in artikel 6 van de Algemene verordening gegevensbescherming.

Identificatie

Zie elektronische identificatie.

Identiteitsleverancier

Een leverancier van een elektronisch identiteitsmiddel.

Informatiestandaard

Een informatiestandaard beschrijft het proces voor een domein en de gegevenselementen die in het proces worden vastgelegd en uitgewisseld.

Informatiestelsel

Het informatiestelsel is een stelsel van afspraken voor het realiseren van veilig en betrouwbaar hergebruik van data.

Knooppunt

Nederlandse vertaling van het Engelse 'node' oftewel een knooppunt in een netwerk. Een .

Leverancier techniek

Een leverancier van software en/of hardware uit de technische architectuur.

Netwerk

Een netwerk van deelnemers. Het netwerk wordt draaiende gehouden door netwerkbeheerders. Zij voeren de governance uit op het netwerk en vertrouwen elkaar op basis van een stelsel van afspraken voor netwerken.

Netwerkactor

Zie actor

Netwerkadres

Het adres binnen de IT-infrastructuur waarop een applicatieservice beschikbaar wordt gesteld. Het adres van een applicatieservice is bijvoorbeeld een URL.

Netwerkbeheerder

Een netwerkbeheerder is een vertrouwde derde partij die namens de netwerkautoriteit rechtspersonen laat deelnemen aan het netwerk overeenkomstig de afspraken. De netwerkbeheerder voert hiervoor de operationele processen uit en hanteert de voorwaarden voor deelname die zijn afgesproken.

Een netwerkbeheerder is in het netwerk eveneens een anker van vertrouwen voor het attesteren van beweringen, waaronder de bewering dat een dienstverlener een deelnemer is van het vertrouwde netwerk.

Netwerkpunt

Een punt in het fysieke netwerk waarop een deelnemer haar diensten beschikbaar stelt of waarvan uit zij gebruik maakt van diensten van andere deelnemers in het netwerk.

Norm

Zie standaard.

Principe

Principes zijn algemene uitgangspunten om inhoud te geven aan de manier waarop het informatieberaad haar missie wil vervullen - het realiseren van een informatiestelsel voor de zorg. Hieronder vallen de basisprincipes en de afgeleide principes.

Publicatie van metadata

Applicatiefunctie voor het publiceren van metadata.

Referentiearchitectuur

Een referentiearchitectuur is een generieke architectuur die richtlijnen en opties geeft om op basis daarvan beslissingen te kunnen nemen tijdens de ontwikkeling van een specifieke architectuur en de implementatie van een oplossing.

Standaard

Een norm of standaard is een document met erkende afspraken, specificaties of criteria over een product, een dienst of een methode.

Bron: Wikipedia.

Subdomein

Een domein binnen een domein.

Toepassingsgebied

Een domein of subdomein.

Toestemming van betrokkene

Toestemming van de betrokkene zoals gedefinieerd in de Algemene verordening gegevensbescherming: elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt.

Validatie

Validatie is het uitvoeren van de controle dat het onderwerp voldoet aan de verwachtingen en de behoeftes van een persoon.

Verificatie

Verificatie is het uitvoeren van de controle dat het onderwerp voldoet aan de gespecificeerde eisen.

Vertrouwd netwerk

Een netwerk van knooppunten die als vertrouwd is aangemerkt.

Verwijsindex

Zie: Gids naar gezondheidsgegevens.

Voorziening

Een voorziening is een product of dienst dat in een behoefte voorzien.

Zorginfrastructuur

Een zorginfrastructuur is het technische ecosysteem dat wordt geïmplementeerd op basis van de juridische, organisatorische, semantische en technische afspraken in een afsprakenstelsel. De zorginfrastructuur moet de veilige en betrouwbare uitwisseling van gegevens tussen deelnemers mogelijk maken.

Wijzigingen

Overzicht van wijzigingen aan de referentiearchitectuur en de wijzigingsprocedure.

1.0.0 - 2019-10

Initiële versie voor het web, getransformeerd vanuit de documenten met de principes en de richtlijnen. Hierbij zijn onderstaande aanpassingen uitgevoerd:

- Tekstuele aanpassingen aan het manifest.
- De diensten zijn geherstructureerd en de richtlijnen voor de diensten herschikt.
- De richtlijnen zijn vernummerd naar de structuur van de diensten.
- Tekstuele toevoegingen voor verheldering van de richtlijnen.

1.1.0 - 2020-03

In deze versie zijn de veranderingen opgenomen naar aanleiding van de reacties op de eerste publicatie en uit de beproeving van de kaders door verschillende programma's. Dit heeft geleid tot de volgende veranderingen:

- Focus op de dingen die belangrijk zijn door korter en krachtiger te communiceren. Dit heeft ertoe geleid dat we de principes ingekort hebben tot het manifest. Er is een vertaaltabel opgenomen om vanuit de principes naar het manifest over te stappen.
- Meer uitleg over de thema's uit het manifest en wat daar mee bedoeld wordt.
- Meer uitleg over het realiseren van vertrouwen tussen de actoren in het netwerk.
- Gelaagdheid in afspraken. We onderkennen afspraken voor vertrouwen, voor technische interoperabiliteit en voor semantische, juridische en organisatorische interoperabiliteit.
- Hanteren van rollen in plaats van diensten.
- Richtlijnen voor interoperabiliteit zijn ingevuld of gaan ingevuld worden door NEN-normen.
- Focus in de richtlijnen op de interactie en de interoperabiliteit tussen actoren. We hanteren geen functionele richtlijnen voor de producten van de leveranciers.
- Focus in de richtlijnen op wat we willen realiseren, niet hoe we dat realiseren.
- Lijst in Excel-formaat opgenomen als checklist en voor pas-of-leg-uit van de uitgangspunten en richtlijnen.

Download DIZRA V2020-03 DIZRA V2020-03.pdf - 2MB

Vertrouwensinfrastructuur

De basis voor het beschikbaar stellen van data en services is vertrouwen. In dit hoofdstuk beschrijven we hoe het vertrouwen wordt opgebouwd.

Inleiding

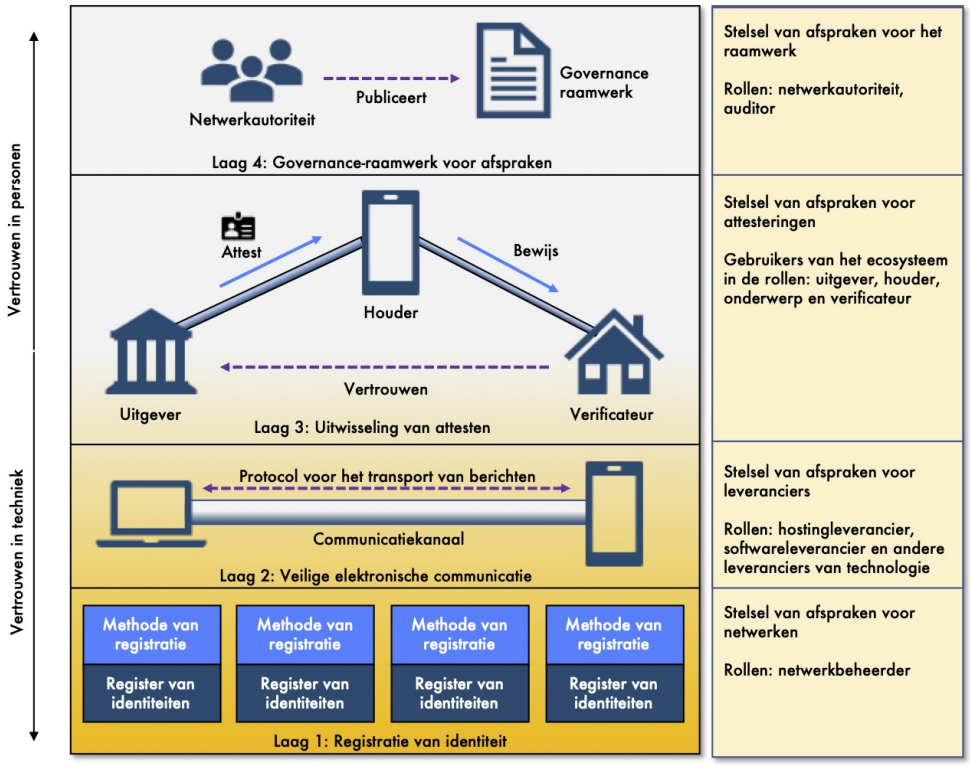
Bob is apotheker. Hij heeft net een verstrekkingsverzoek ontvangen van Alice voor een geneesmiddel op recept. Hij kent de voorschrijver niet. Om het geneesmiddel te mogen verstrekken moet Bob verifiëren dat de voorschrijver bevoegd is om een recept voor te schrijven. Het informatiesysteem van Bob verifieert de bevoegdheid en meldt dat de voorschrijver bevoegd is. Hij verstrekt de medicatie daarom aan Alice.

Het vertrouwen van Bob is geen automatisme. Bob moet geloof hebben in het systeem van verifiëren. Aan de hand van de casus van Bob en Alice beschrijven we hieronder de stappen die nodig zijn om het vertrouwen in het systeem te verkrijgen.

In het systeem onderkennen we 4 lagen waarmee het vertrouwen wordt opgebouwd. We tellen de lagen van beneden naar boven.

1. De eerste laag is de laag waarmee we personen, maar ook apparaten en dingen kunnen identificeren. Zodat Bob en Alice elkaar kunnen identificeren, maar natuurlijk ook de voorschrijver. Dit is Caroline. De actoren moeten elkaar uniek kunnen identificeren.
2. Met de tweede laag zorgen we ervoor dat Bob, Alice en Caroline berichten kunnen verzenden en veilig met elkaar kunnen communiceren.
3. In de derde laag moeten we ervoor zorgen dat Bob vertrouwen heeft dat Caroline een bevoegde voorschrijver is. Ook al verkrijgt Bob het verstrekkingsverzoek van Alice.
4. Om het vertrouwen in de derde laag te verkrijgen is de vierde laag nodig, namelijk de laag met het raamwerk aan afspraken. Dat wat we ook wel een afsprakenstelsel noemen. Er zijn bijvoorbeeld afspraken nodig hoe we verifiëren dat we een persoon kunnen vertrouwen.

De lagen zijn in het onderstaande figuur weergegeven en worden vervolgens hieronder beschreven. Het model is overgenomen uit de volgende specificatie: "The Trust Over IP Stack".



Figuur 1: Lagen van vertrouwen in techniek en in personen

Laag 1: Registratie van identiteit

In de eerste laag borgen we de identificatie. Hierbij is van toepassing dat alles een identiteit kan hebben. Meer en meer is de uitgever van een gegevenselement een apparaat. En kunnen apparaten of andere dingen ook het onderwerp zijn van gegevens. Bijvoorbeeld als we gegevens registreren over de betrouwbaarheid van een bloeddrukmeter of een ander apparaat. Het gaat met andere woorden niet alleen over de identiteit van personen. Iedere actor moet een identiteit kunnen krijgen. Dit is overigens een anonieme identificatie zonder betekenis.

Een actor kan haar identiteit in een netwerk registreren. Alles wat producent is van data moet een identiteit registreren als de data van die producent verifieerbaar moet zijn. We zien in de praktijk meerdere netwerken met daarin meerdere nodes (knooppunten). Zo kan er een netwerk zijn voor gemeenten, een netwerk voor apparaten, een regionaal netwerk of een onderzoeksnetwerk. Iedereen kan zelf haar netwerk kiezen. Eenieder heeft keuzevrijheid.

> **Bob, Alice en Caroline hebben al vele identiteiten.**
>
> - Bob, Alice en Caroline hebben allen een Burgerservicenummer.
> - Bob als apotheker en Caroline als huisarts zijn beiden BIG-geregistreerd en hebben een BIG-nummer.
> - Bob en Caroline moeten kunnen declareren bij de zorgverzekeraar van Alice. Daarom hebben ze een AGB-nummer, evenals de apotheek en huisartsenpraktijk.
> - Daarnaast hebben de apotheek en de huisartsenpraktijk een KvK-nummer in het Handelsregister.
>
> We hebben dus al vele identiteiten als rechtspersoon en als natuurlijk persoon.

Denken vanuit de identiteit

Een identiteit ontvangen we meestal vanuit een organisatie, een rechtspersoon. We hebben als persoon daarom vele identiteiten. Organisaties kijken en denken namelijk vanuit hun eigen bedrijfsvoering naar de personen om hun heen. Zowel naar rechtspersonen als natuurlijke personen en identificeren die personen met een nummer. Een organisatie staat in deze denkwijze centraal. Deze denkwijze is echter niet houdbaar als we naast personen ook een identiteit nodig hebben voor apparaten en andere dingen. Dan creëren we chaos door de vele identiteiten die in omloop zijn.

We willen een persoon centraal stellen, maar ook het apparaat en andere dingen. Het is veel natuurlijk om te zeggen dat iedere persoon, ieder apparaat en ding een eigen identiteit heeft. In de fysieke wereld is dit normaal. In de virtuele wereld moet het daarom ook normaal zijn om deze denkwijze te hanteren. De identiteit van een organisatie gebruiken we in de fysieke wereld contextueel. We authenticeren ons contextueel. Bijvoorbeeld via een paspoort of via een OV-kaart. In de virtuele wereld moeten we onszelf ook contextueel kunnen identificeren en authenticeren. Uitgangspunt is daarom dat alles een eigen identiteit heeft en dat eenieder contextueel andere elementen kan gebruiken.

> **Wat betekent dit voor Bob, Alice en Caroline?**
>
> We maken onderscheid tussen natuurlijke personen en rechtspersonen. Iedere persoon moet een netwerk kiezen waarop zij hun identiteit aanmaken. Bob en Caroline maken in het voorbeeld gebruik van een netwerk van zorgverleners waarin zij een identiteit hebben aangemaakt voor zichzelf, maar ook voor de apparaten die zij gebruiken en hun huisartsenpraktijk en apotheek.
>
> Een netwerk wordt geïmplementeerd en operationeel gehouden door netwerkbeheerders. Iedere netwerkbeheerder heeft een eigen knooppunt (node) in het netwerk. Het netwerk zorgt

> voor de registratie van de elementen waarmee data kan worden geverifieerd op herkomst, integriteit en geldigheid. Het netwerk registreert deze elementen onveranderbaar en gedistribueerd over alle knooppunten. Hiermee worden beveiligingsrisico's gespreid en de kwetsbaarheid van één registratie voorkomen. Deze structuur wordt een 'Identity Trust Fabric' genoemd (bron: Gartner).
>
> Bob en Caroline kiezen ieder een netwerkbeheerder als beheerder van hun publieke identiteit. Bob kiest voor Acme en Caroline voor Faber. Alice maakt gebruik van een applicatie van Stark. Zij registreert haar identiteit niet omdat ze deze privaat wil houden. Alleen uitgevers van een attest moeten een publieke identiteit hebben.
>
> Ieder netwerk heeft haar eigen stelsel van afspraken. Hierin wordt afgesproken:
>
> - De governance op het netwerk en de wijze van samenwerking. Met als uitkomst dat de netwerkbeheerders elkaar vertrouwen.
> - De voorwaarden voor registratie van een identiteit. Een netwerk kan open zijn voor iedereen, maar er kunnen ook voorwaarden gespecificeerd zijn waaraan een persoon moet voldoen. In het voorbeeld is een netwerk geïmplementeerd voor zorgverleners waaraan alleen erkende zorgverleners mogen meedoen.
> - De netwerken die vertrouwd zijn. Het netwerk van Bob en Caroline moet bijvoorbeeld het netwerk van Alice vertrouwen.

Een afspraak over de methode van registratie is noodzakelijk zodat bijvoorbeeld het netwerk herkend kan worden waarin de identiteit is aangemaakt. Het moet ook borgen dat een identiteit uniek is.

Laag 2: Veilige elektronische communicatie

Caroline is de voorschrijver van het geneesmiddel en heeft het verstrekkingsverzoek gemaakt. Caroline moet het bericht met het verstrekkingsverzoek veilig elektronisch kunnen communiceren met Alice, dan wel rechtstreeks met Bob. Veilige communicatie bestaat enerzijds uit een veilig communicatiekanaal en anderzijds uit een protocol voor het transport van berichten.

Een veilig communicatiekanaal

Een communicatiekanaal is veilig als:

1. Berichten zijn versleuteld;
2. Het communicatiekanaal is aangemaakt tussen de elektronische vertegenwoordigers van de actoren die met elkaar willen communiceren.

Een oplossing voor het versleutelen van berichten is het gebruik van Transport Layer Security (TLS). Dit protocol is gebaseerd op een Public Key Infrastructuur (PKI) met uitgifte en beheer van certificaten. Certificaten kunnen echter niet voor iedere toepassing worden gebruikt. Een toepassing met mobiele apparaten of met dingen in de context van "The Internet of Things" zijn niet mogelijk of zeer kostbaar als deze met PKI moeten worden opgelost. Een Decentralized Public Key Infrastructure (DPKI) heeft deze nadelen niet.

Zowel PKI als DPKI borgen dat met de juiste elektronische vertegenwoordiger wordt gecommuniceerd door aan te tonen dat de vertegenwoordiger controle heeft over de private sleutel van de persoon. DPKI heeft echter als voordeel dat het volledig anoniem is waar anonieme communicatie van berichten gewenst of noodzakelijk is.

> **Wat betekent dit voor Bob, Alice en Caroline?**
>
> Een veilig communicatiekanaal stelt Bob, Alice en Caroline in staat om met elkaar te communiceren. Zij zien niet of het veilig is of niet. Ze moeten vertrouwen dat het veilig is.

> Hiervoor zijn afspraken nodig tussen de technische leveranciers die de communicatiekanalen veilig moeten maken. Door certificering van de leveranciers die voldoen aan de afspraken kunnen Bob, Alice en Caroline zien dat de techniek die zij gebruiken veilig is. Voor deze certificering is een een stelsel van afspraken nodig voor leveranciers van techniek.

Een protocol voor het transport van berichten

Voor het transport van berichten zijn er meerdere protocollen beschikbaar. Ieder protocol is gemaakt met een doel voor ogen. HTTP is een van de meest bekende protocollen, maar er zijn er meer. Naast het protocol zijn er standaarden voor het transport van berichten. Zo zijn er meerdere standaarden die berichten verzenden over HTTP. Ten aanzien van het protocol en de standaard is er geen "One Size Fits All"-oplossing. Voor iedere toepassing moeten we op zoek gaan naar het juiste protocol en standaard.

> **Wat betekent dit voor Bob, Alice en Caroline?**
>
> Een protocol en een standaard voor het verzenden en ontvangen van berichten is iets wat Bob, Alice en Caroline niet zien. Zij willen gewoon met elkaar kunnen communiceren. Veilige communicatie moet echter niet beperkend zijn in de toepassingsmogelijkheden. In onderstaand voorbeeld beschrijven we een toepassing.
>
> Bob heeft een apparaat op de balie staan. Alice houdt haar telefoon tegen het apparaat aan en bevestigt dat zij het verstrekkingsverzoek wil communiceren. Bob ziet dat zijn informatiesysteem het verstrekkingsverzoek heeft ontvangen. Het is een voorbeeld van een communicatiekanaal en een protocol voor transport van berichten die specifiek is voor de toepassing.

Laag 3: Uitwisseling van attesten

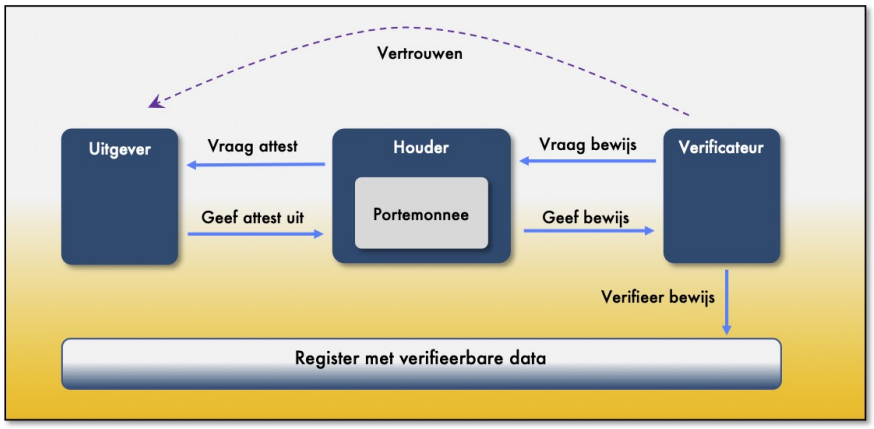
De eerste twee lagen zijn nodig voor de uitwisseling van gegevens. Pas in de uitwisseling van attesten wordt betekenis gegeven aan de data en aan de manier waarop de data kan worden geverifieerd.

Attest als elektronische verklaring die een bewering ondersteunt

Een attest is een elektronisch bewijs, een (officiële) verklaring die een mondelinge bewering versterkt, ondersteunt, wettigt (Wikipedia). We kunnen alle data als bewering zien. Alice beweert bijvoorbeeld dat zij een verstrekkingsverzoek heeft voor de verstrekking van geneesmiddelen. Bob moet deze bewering geloven. Naast de beweringen van anderen kunnen we ook zelf beweringen doen of kunnen dingen beweringen doen. De vraag is iedere keer of we de bewering moeten geloven. Kunnen we de bewering vertrouwen? Met een attest bedoelen we een verifieerbare bewering zodat we deze kunnen vertrouwen.

In onderstaand figuur zijn de stappen voor het uitgeven van een attest en het overhandigen van bewijs weergegeven.

1. De uitgever geeft het attest uit, al dan niet op basis van een vraag.
2. De verklaring wordt uitgegeven aan een de houder. De houder bewaart het attest in haar portemonnee.
3. Voor het uitvoeren van een transactie met de verificateur kan deze om bewijs vragen. De houder geeft het bewijs aan de verificateur. Het bewijs is gebaseerd op het attest, maar aangepast aan wat minimaal noodzakelijk is.
4. De verificateur moet de verklaring kunnen verifiëren. De verklaring is autonoom in haar bewijsvoering. Dit betekent dat bewijsvoering niet afhankelijk is van de wijze waarop de verklaring bezorgd is.

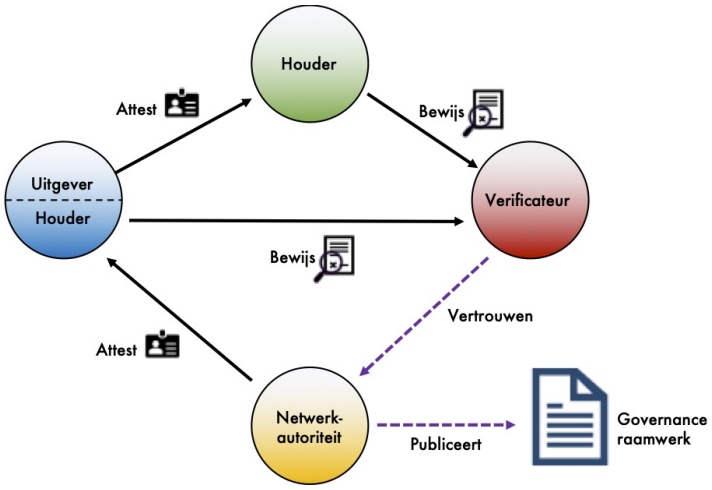


Figuur 2: Rollen voor verifieerbaar elektronisch bewijs

Vertrouwen hebben in het bewijs

De verificateur moet besluiten of zij de verklaring aanneemt als bewijs. Zij zal de verklaring moeten geloven en vertrouwen. De manier waarop dit vertrouwen wordt verkregen moet zijn afgesproken. Vanuit de afspraken moet de uitgever zijn aangewezen als geloofwaardig. Een register met data waardoor beweringen verifieerbaar zijn ondersteunt hierin. Het biedt eveneens de mogelijkheid de geldigheid van een attest te verifiëren. Een register met verifieerbare data zien we als onderdeel van de vertrouwensdiensten van een netwerkbeheerder.

De techniek kan controleren dat een attest aan alle eisen voldoet. De techniek kan echter niet controleren dat de actor die het attest heeft ondertekend ook vertrouwd moet worden. Hiervoor zijn aanvullende afspraken nodig over de uitgevers die vertrouwd zijn, dan wel aan welke kenmerken zij moeten voldoen om vertrouwd te zijn. Zij kunnen bijvoorbeeld vertrouwd zijn omdat zij een attest van de netwerkautoriteit hebben ontvangen of van een andere autoriteit. Maar het blijft noodzakelijk dat minimaal één uitgever vertrouwd wordt in het netwerk.



Figuur 3: Afspraken als onderdeel in de driehoek van vertrouwen

Wat betekent dit voor Bob, Alice en Caroline?

Caroline is auteur en uitgever van het verstrekkingsverzoek. Het is een van de onderdelen van het recept dat ze aan Alice heeft voorgeschreven. Caroline heeft het recept uitgegeven aan Alice. Alice is daarmee de houder van het attest. Met het verstrekkingsverzoek gaat Alice naar een apotheek en overhandigt elektronisch het verstrekkingsverzoek.

Bob is apotheker. Hij heeft net het verstrekkingsverzoek ontvangen van Alice voor een geneesmiddel op recept. Hij kent de Caroline niet. Om het geneesmiddel te mogen verstrekken moet Bob verifiëren dat de Caroline bevoegd is om een recept voor te schrijven. Het informatiesysteem van Bob controleert het volgende:

1. Dat het verstrekkingsverzoek elektronisch ondertekent is door de identiteit van de uitgever;
2. Dat de gegevenselementen in het verstrekkingsverzoek niet veranderd zijn gedurende het transport;
3. Dat de uitgever opgenomen is in het BIG-register;
4. Dat de uitgever is aangemerkt als bevoegde voorschrijver van geneesmiddelen.

Het informatiesysteem meldt dat Caroline bevoegd is. Bob verstrekt de medicatie aan Alice.

In ons voorbeeld bezorgt Alice het verstrekkingsverzoek bij Bob. De bezorging kan echter ook rechtstreeks vanuit Caroline naar Bob. Het attest en de bewijsvoering is daarom onafhankelijk van het kanaal van bezorging.

Een verwerking verantwoorden

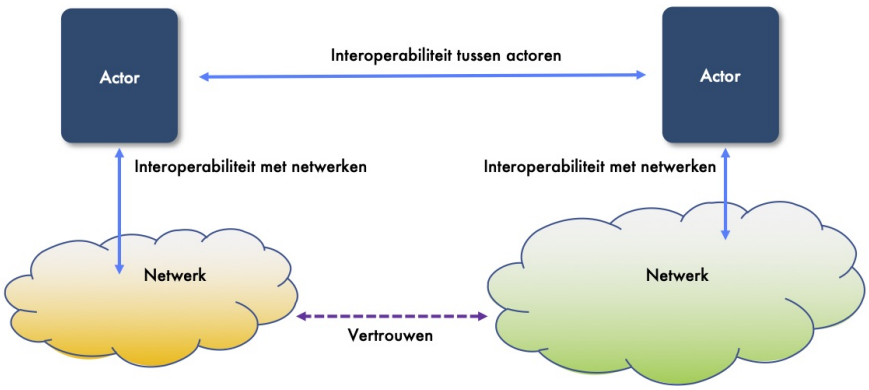
Bob zal de verwerking van persoonsgegevens moeten kunnen verantwoorden. Net als dat hij de verstrekking van een geneesmiddel moet kunnen verantwoorden. Ongeacht het kanaal waarmee het bericht bij hem terecht is gekomen zal hij de verantwoording moeten kunnen uitvoeren.

Laag 4: Governance-raamwerk voor afspraken

In een governance-raamwerk wordt het vertrouwen afgesproken. Ieder netwerk maakt afspraken en heeft een governance-structuur waarmee de afspraken worden beheerd. We spreken over een raamwerk omdat op iedere laag afspraken kunnen worden gemaakt die zelfstandig ontwikkeld, geïmplementeerd en beheerd worden. Het geheel aan afspraken borgt het vertrouwen.

1. **Afspraken met netwerkbeheerders.** Dit specificeert de afspraken voor het netwerk met de structuur voor het registreren van data waarmee een attest kan worden geverifieerd.
2. **Afspraken met leveranciers van techniek**. Hierin wordt afgesproken hoe de leveranciers van de onderdelen in de vertrouwensinfrastructuur (zoals hostingpartijen, leveranciers van software en hardware) kunnen worden geverifieerd en worden gecertificeerd.
3. **Afspraken over het vertrouwen in uitgevers van attesten.** Het betreft afspraken over welke uitgevers worden vertrouwd en welke regels zij moeten hanteren bij het uitgeven en intrekken van attesten.
4. **Afspraken voor het gehele ecosysteem** waarin afspraken worden gemaakt om vertrouwen en interoperabiliteit tussen de netwerken te borgen.

Natuurlijke personen, rechtspersonen en dingen maken gebruik van de vertrouwensinfrastructuur van een netwerk. Zij zijn echter niet gebonden aan een netwerk.



Figuur 4: Afspraken over interoperabiliteit en vertrouwen

Een zorgaanbieder in de langdurige zorg heeft bijvoorbeeld te maken met verschillende netwerken zoals een netwerk voor de langdurige zorg, van gemeenten, voor hulpmiddelen, onderzoek, huisartsen etc. De netwerken moeten daarom afspraken maken over interoperabiliteit en afspreken welke netwerken zij vertrouwen.

Regie op gezondheidsdata

Het eerste principe in het manifest is regie op gezondheidsgegevens voor burgers. In dit hoofdstuk beschrijven we de uitgangspunten voor dit thema.

Wat is regie op gezondheidsdata?

Regie op gezondheidsdata staat voor het vrije verkeer van persoonlijke gegevens onder regie van mensen zelf. We hanteren voor de zorg de term gezondheidsdata, maar het betreft regie op gegevens in het algemeen. We denken namelijk dat gezondheidsdata niet alleen medische gegevens betreft, maar alle gegevens die binnen de zorg relevant zijn.

We kijken naar het programma regie op gegevens voor de definitie van regie op gegevens. In het programma regie op gegevens heeft de overheid samen met private en maatschappelijke organisaties uitgewerkt hoe dit plaats moet vinden (zie: https://kennisopenbaarbestuur.nl/thema/regie-op-gegevens/.

Regie op gegevens als principe maakt onderdeel uit van het regeerakkoord, de digitalisering-strategie 'Nederland Digitaal' en de digitale agenda 'NLDIGIbeter'.

> *"Regie op gegevens hanteert als vertrekpunt dat mensen inzage moeten hebben in hun persoonlijke gegevens en het gebruik daarvan door derden, dat zij de mogelijkheid moeten hebben om gegevens te corrigeren of verwijderen en -niet in de laatste plaats- dat zij gegevens moeten kunnen (her)gebruiken, zowel binnen de overheid als daarbuiten. Hierdoor verbetert de transparantie, neemt de kwaliteit van gegevens toe en wordt de positie van de burger versterkt. Voor burgers en bedrijven zorgt het voor lastenverlichtingen en het optimaliseren van processen. Persoonlijk datamanagement draagt bij aan transparantie, inzage en correctie, digitale zelfbeschikking, privacy, dataminimalisatie, de kwaliteitsverbetering van gegevens en zelfredzaamheid van mensen. Daarmee is PDM tevens een uitwerking van de beginselen zoals die gehanteerd worden bij 'privacy by design' en 'security by design'."*
>
> Bron: Greenpaper Regie op gegevens, inleiding
>
> Toelichting: PDM staat voor Persoonlijk datamanagement

Vanuit het programma zijn de volgende principes gespecificeerd (zie infographic):

- **Inclusiviteit**: Mensen met persoonlijke verschillen in mogelijkheden, omstandigheden en culturen nemen vrijelijk deel aan het (digitale) maatschappelijk leven.
- **Mens centraal**: Mensen krijgen meer grip op het leven door regie op eigen persoonlijke gegevens.
- **Digitale autonomie**: Personen verstevigen hun positie door vergroten van inzicht in en invloed op persoonlijk gegevensverkeer.

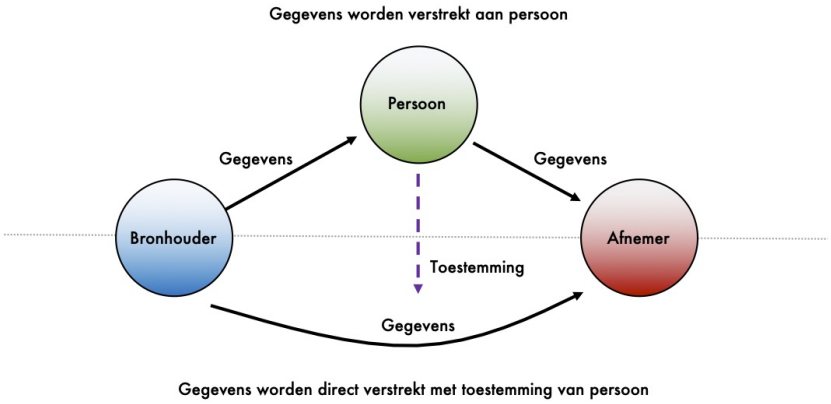
Om de bovenstaande principes te realiseren is transparantie noodzakelijk. Transparantie over de intenties en het gedrag van personen, aanbieders van data en afnemers. Daarnaast vormen interoperabiliteit, vertrouwen en dataminimalisatie de ingrediënten voor regie op gegevens.

De principes voor regie op gegevens komen overeen met de uitgangspunten voor regie op gegevens die door de community van IT-Architecten zijn geuit en in eerdere publicaties zijn verwoord.

Vormen van regie

Er zijn twee vormen van regie op gegevens. De eerste vorm is dat de bronhouder de gegevens verstrekt aan de persoon. Het is vervolgens aan de persoon zelf om deze gegevens door te zenden naar afnemers.

De tweede vorm is dat de bronhouder de gegevens direct verstrekt aan de afnemer, met toestemming van de persoon.



Figuur 1: Vormen van regie op gegevens

In maart 2019 is het kader voor regie op gegevens door het programma gepubliceerd. In het kader zijn drie horizonnen beschreven in de ontwikkeling van het principe 'regie op gegevens'.

1. **Bronhouders stellen gegevens ter beschikking** waarbij een persoon een kopie ontvangt van een dataset.
2. **Bronhouders maken gegevens toegankelijk** voor een persoon. Ze werken mee aan de uitwisseling van gegevens onder regie van een persoon. Een persoon kan aangeven dat partij A een specifiek gegeven of een set van gegevens mag inzien bij partij B voor een bepaald doel en voor een bepaalde duur.
3. **Een persoon heeft volledig zelf de regie over zijn of haar eigen gegevens**. Als persoon doe je een bewering (ik ben 18, ik heb mijn rijbewijs) en een bevoegde instantie attesteert deze bewering.

DIZRA geeft in de richtlijnen ondersteuning aan regie op gegevens overeenkomstig de visie uit het kader.

> **Wat betekent dit voor burgers, patiënten en cliënten?**
>
> Alice is gevallen op straat. Ze viel over een randje en kwam op straat lelijk ten val op haar schouder. Een aantal omstanders kwam haar te hulp. Super lief en het gaf haar een warm gevoel ondanks de pijn van haar val. De ambulance is gebeld en even later was ze onderweg naar het ziekenhuis. In het ziekenhuis bleek dat Alice haar schouder uit de kom was. Het werd snel gezet en ze mocht naar huis.
>
> Zelf regie op gegevens hebben betekent voor Alice dat:
>
> - Dat ze een attest ontvangt dat er een foto is gemaakt. Alice kan deze foto delen.
> - Dat ze een attest ontvangt dat ze een doorverwijzing heeft. Met het attest kan ze naar de traumapoli in het ziekenhuis bij haar in de buurt. De bewering dat ze een doorverwijzing heeft is geattesteerd door een bevoegde arts.

Wat als mensen digitaal niet mee kunnen of willen doen?

DIZRA gaat over digitale en elektronische vindbaarheid, toegankelijkheid, interoperabiliteit en hergebruik van data binnen de gezondheidszorg en regie. Vertrouwen en regie op gegevens zijn hierbij belangrijke uitgangspunten. Een belangrijk onderdeel van toegankelijkheid is: iedereen kan meedoen in de (digitale) samenleving. Dit noemen we 'digitale inclusie'.

Voor meer informatie over digitale inclusie verwijzen we naar: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/toegankelijkheid/digitale-inclusie/

Gemeenschappelijke taal

In dit hoofdstuk behandelen we het thema voor een gemeenschappelijke taal en terminologie.Moeten we allemaal dezelfde taal spreken?

Wanneer spreek je een gemeenschappelijke taal?

Een gemeenschappelijke taal spreken betekent dat je elkaar begrijpt binnen de context van een onderwerp. Een gemeenschappelijke taal spreek je als we binnen een context een ontologie hebben en een vocabulaire. In de onderstaande beschrijving maken we gebruik van: Ontological Foundations for Structural Conceptual Models van Giancarlo Guizzardi.

Wat is een context?

Het afspreken van een gemeenschappelijke taal en terminologie vereist een contextueel kader. De context bepaalt namelijk de taal en de terminologie die we hanteren. Een context zien we in DIZRA als een situatie waarover afspraken worden gemaakt en wat betrekking heeft op een persoon of haar omgeving.

Voorbeelden van context:

- Fysieke context (locatie, tijd etc.)
- Omgevingscontext (temperatuur, hoogte, licht etc.)
- Informatiecontext (geneesmiddel, diagnose, personeel etc)
- Persoonlijke context (gezondheid, gesteldheid, activiteiten etc.)
- Sociale context (groepsactiviteit, sociale relaties etc.)
- Applicatiecontext (e-mail, bezochte websites etc.)
- Systeemcontext (netwerkverkeer, status van de printer etc.)

DIZRA hanteert als uitgangspunt dat we data modelleren voor een informatiecontext. De andere contexten zijn onderdeel van het model. Voorbeelden van een informatiecontext zijn medicatie, verpleging, zwangerschap en geboorte en beelden. De informatiecontext vormt het kader waarvoor we de ontologie ontwikkelen. Dat zorgt ervoor dat we grenzen stellen aan wat we modelleren. Maar ook dat we modelleren wat bij elkaar hoort. Maar de grens goed bepalen is complex. We zullen daarin moeten leren en moeten kunnen veranderen.

Wat is een ontologie en vocabulaire?

Om informatie uit data te halen is een interpretatie nodig. De interpretatie geeft betekenis aan data. Ontologie geeft betekenis aan data, aan de concepten die we in de werkelijkheid zien. Een ontologie is een beschrijving van het domein in de taal van het domein. Een vocabulaire is de verzameling woorden die we gebruiken in de ontologie.

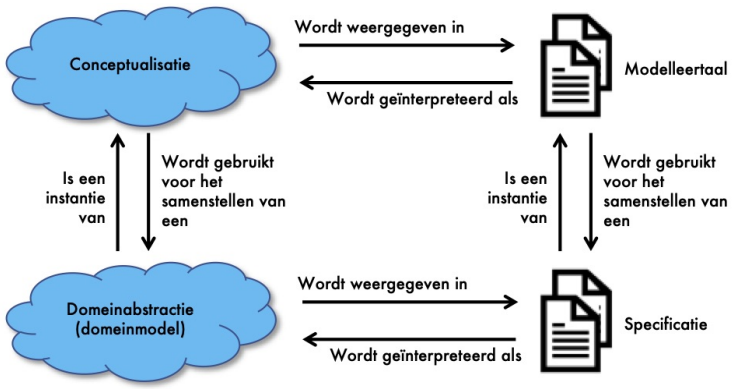
> **Ontologie in de praktijk**
>
> Als we "14-2" zien dan kunnen we denken aan 14 februari, aan Valentijnsdag. In beide gevallen denken we echter aan het concept van een datum als de we data bekijken. Het concept datum kan op verschillende manieren worden weergegeven. Met een datumnotatie, maar ook als een dag met betekenis. Met de representatie geven we de wijze aan waarop de data wordt opgeslagen of wordt weergegeven.
>
> "14-2" is data. We hebben onderkend dat het een datum is. Maar nu willen we weten wat "14-2" betekent. Het moet informatie worden. Is het de verjaardag van een persoon, de datum waarop zij met vakantie gaat of de begindatum van haar nieuwe baan?

> Ontologie is zinsontleding. We moeten eerst de zin beschrijven. Een zin is opgebouwd uit een onderwerp, een predicaat (of gezegde) en het voorwerp. We beschrijven daarom: Alice is jarig op "14-2". Hiermee geven we betekenis aan "14-2" en kunnen we de data interpreteren. Maar daarmee zijn we er nog niet. Als mens weten we wat een verjaardag is, maar een machine weet dat niet. We zullen het concept "verjaardag" moeten uitleggen aan de machine. Je kunt zeggen dat iemand geboren is op die datum. Maar kent een machine het concept "geboren"?

Data meervoudig kunnen gebruiken en machineleesbaar maken betekent dat we de huidige data moeten schonen. Het moet met name geschoond worden van arbitraire definities van data. De concepten moeten eenduidig geïnterpreteerd kunnen worden. De data zal onze kennis moeten beschrijven van concepten.

Ontologie en zorginformatiebouwstenen (zibs)

We zien zorginformatiebouwstenen als een specificatie die gemaakt is op basis van een ontologie. Een ontologie specificeert de betekenis van een concept. Het is een conceptualisatie van de werkelijkheid.



Figuur 1: Relatie tussen conceptualisatie van een ontologie en een domeinabstractie

Een zorginformatiebouwsteen beschrijft een zorginhoudelijk concept in termen van de gegevenselementen waaruit dat concept bestaat, de datatypes van die gegevenselementen etc. Het is met andere woorden een abstractie van de ontologie.

Data bij de bron

Wat bedoelen we met data bij de bron? In dit hoofdstuk behandelen we dit thema en de wijze waarop een organisatie invulling kan geven aan het uitgangspunt van data bij de bron.

Wat bedoelen we met data bij de bron?

Met data bij de bron geven we invulling aan een decentrale informatiehuishouding. De minister stelt dat hij hecht aan verantwoord gebruik van data en het - waar mogelijk - voorkomen van landelijke dataverzamelingen. Bron: Bijlage Kamerbrief over data laten werken voor gezondheid - Data laten werken voor gezondheid, 15 november 2018. Dit is in de richtlijnen opgenomen.

Verantwoord beheer en gebruik van data

De minister stelt dat elke bronhouder zich verantwoordelijk dient te gedragen als rentmeester. Maar wat is een rentmeester in de context van persoonsgegevens? Een rentmeester is verantwoordelijk voor de bescherming van een persoon. De persoon die het onderwerp is van de data. De rentmeester heeft deze data in beheer gekregen van de persoon. Een rentmeester handelt als zodanig. Een rentmeester draagt zorg voor een verantwoord beheer en gebruik van data. Dit in brede zin.

De rentmeester handelt niet alleen in het belang van een persoon. Zij handelt met toestemming van de persoon ook in het algemeen belang van gezonde mensen en vanuit het maatschappelijk nut. De rentmeester doet dit door data verantwoord en gecontroleerd beschikbaar te stellen. Hierdoor wordt kennis gedeeld en waarde gecreëerd voor alle mensen. Data wordt alleen beschikbaar gesteld als de persoon toestemming heeft gegeven. Dit moet in het ontwerp van de data zijn opgenomen ("consent by design").

Een duurzaam rentmeesterschap is de basis voor diverse technologische toepassingen.

> **Wat betekent rentmeesterschap?**
>
> Een bronhouder mag zich rentmeester noemen als zij voldoet aan de volgende regels:
>
> 1. Een rentmeester denkt vanuit het belang van de persoon en het maatschappelijk belang.
> 2. Het rentmeesterschap omvat beleidsrichtlijnen, organisatievisie, -missie en –strategie en een aangepaste inrichting van processen, technologie en governance.
> 3. Een rentmeester voert een of meer delen van het rentmeesterschap uit.
> 4. Een rentmeester heeft persoonlijke data in beheer gekregen volgens vastomlijnde afspraken en beginselen, met het oog op persoonlijk en maatschappelijk welzijn en gezondheid. Data in vertrouwen.
> 5. Een rentmeester weet dat met betrouwbare data waarde kan worden gecreëerd.
> 6. Een rentmeester zorgt ervoor dat de persoon regie heeft en behoudt op zijn of haar gegevens ("consent by design").
> 7. De rentmeester beheert de data zodat waarde kan ontstaan. In eerste instantie voor de zorg en het welzijn van de persoon zelf en verder voor de zorg en het welzijn van de gemeenschap en het collectief belang.
> 8. De rentmeester hanteert diverse algemeen aanvaarde principes zoals zeggenschap, interoperabiliteit, FAIR-data (zowel technisch als functioneel), datasolidariteit en digitale inclusie. Het zijn principes voor een op waarde gestuurde gezondheidszorg.
> 9. De rentmeester zorgt ervoor dat een persoon altijd toegang heeft tot zijn of haar data. Uitgangspunt is en blijft dat waar data ter beschikking wordt gesteld, dit onder regie en zeggenschap van de betrokken persoon zelf gebeurd.

Zoals de minister in zijn brief heeft aangegeven is voor het gebruik van data vertrouwen nodig en regie op gegevens door de persoon. Het vertrouwen dat door het proces rentmeesterschap en de rol van rentmeester wordt bewaakt.

Gelijk speelveld

In dit hoofdstuk beschrijven we wat een gelijk speelveld voor leveranciers is. Wat bedoelen we daarmee en waarom is dat belangrijk?

Wat is een gelijk speelveld?

Volgens de Autoriteit Consument en Markt is een eerlijk speelveld een speelveld waarin de kansen en keuzes van consumenten en andere bedrijven niet worden belemmerd. Een gelijk speelveld zien we ook als een marktsituatie (een speelveld) waar dezelfde regels gelden voor alle leveranciers, waardoor zij een gelijke uitgangspositie hebben om met elkaar te concurreren. Een gelijk speelveld waarin ook voor nieuwe toetreders kansen bestaan om te concurreren.

DIZRA hanteert de richtlijn dat er alleen afspraken mogen worden gemaakt over het gebruik van open (internationale) standaarden, maar niet over het gebruik van producten of diensten van een leverancier. We bedoelen hier de standaarden, producten en diensten die in de technische zorginfrastructuur afgesproken worden.

Een keuze voor een product of dienst van een leverancier als afspraak belemmert de vrijheid van keuze van natuurlijke personen en rechtspersonen binnen de gezondheidszorg. In de afspraken mogen geen belemmeringen worden opgelegd. Een zorgaanbieder moet een vrije keuze hebben voor een leverancier en geen gedwongen keuze.

Waarom is een gelijk speelveld belangrijk?

De Mededingingswet verbiedt afspraken waardoor de mededinging op de Nederlandse markt of een deel daarvan wordt verhinderd, beperkt of vervalst. Een keuze voor een leverancier in een stelsel van afspraken mag daarom niet. Naast dat het niet mag willen we het ook niet. We herkennen de situaties dat de macht bij de leveranciers ligt maar al te goed. We weten welke gevolgen dat heeft.

Een eerlijk speelveld tussen leveranciers moet de concurrentie stimuleren en voorkomen dat de macht bij de leverancier komt te liggen. Concurrentie is de prikkel tot doelmatig en doeltreffend werken. Concurrentie moet leveranciers inwisselbaar maken en aanzetten tot nieuwe en betere dienstverlening.

Een eerlijk speelveld moet zorgen voor een breed veld van leveranciers die innovatie brengen. Dit is nodig om tot innovatie te komen voor nieuwe en betere dienstverlening. Een monocultuur van leveranciers betekent dat innovatie steeds vanuit dezelfde leveranciers moet komen. We weten dat dit het vermogen tot innoveren verlaagd. Een monocultuur is daarom niet gewenst.

Duurzaam

In dit hoofdstuk beschrijven we het begrip duurzaam. Waneer kunnen we het informatiestelsel duurzaam noemen?

Wat is duurzaam?

Een van de gewenste uitkomsten is een duurzaam informatiestelsel in de zorg. Maar wat is duurzaam in een wereld die continue veranderd? Dat is de verandering zelf. Om duurzaam te zijn moeten we een hoog vermogen tot veranderen realiseren. We weten uit ervaring dat het vermogen tot veranderen wordt verhoogd als we het aantal afhankelijkheden verlagen.

Onafhankelijke informatiestandaarden

Duurzaamheid gaat over de inrichting van het informatiestelsel en de wijze waarop standaarden worden gehanteerd. Een duurzaam informatiestelsel wordt gerealiseerd als we vanuit autonome onderdelen denken.

Een informatiestandaard beschrijft het proces voor een domein en de gegevenselementen die in het proces worden vastgelegd en uitgewisseld. Iedere informatiestandaard moet autonoom zijn om te kunnen veranderen.

Onafhankelijke ontologie

DIZRA hanteert als uitgangspunt dat we niet alle data gemeenschappelijk kunnen beschrijven in een ontologie. Een ontologie zal in veel gevallen worden meegeleverd door een leverancier. Een leverancier van een röntgenapparaat levert de ontologie van dat apparaat. Hopelijk gestandaardiseerd in een samenwerking tussen leveranciers van röntgenapparaten.

Uitgangspunt is dat iedereen een ontologie kan leveren. De ontologie moet gebruikt kunnen worden in het informatiestelsel. Iedere ontologie is autonoom en kan zelfstandig veranderen in een proces die we zelf niet onder controle hebben. We hebben alleen de controle over het toepassen van een ontologie en de manier waarop we zelf data beschikbaar stellen aan anderen. Dat willen we zoveel mogelijk doen op basis van een gemeenschappelijke ontologie.

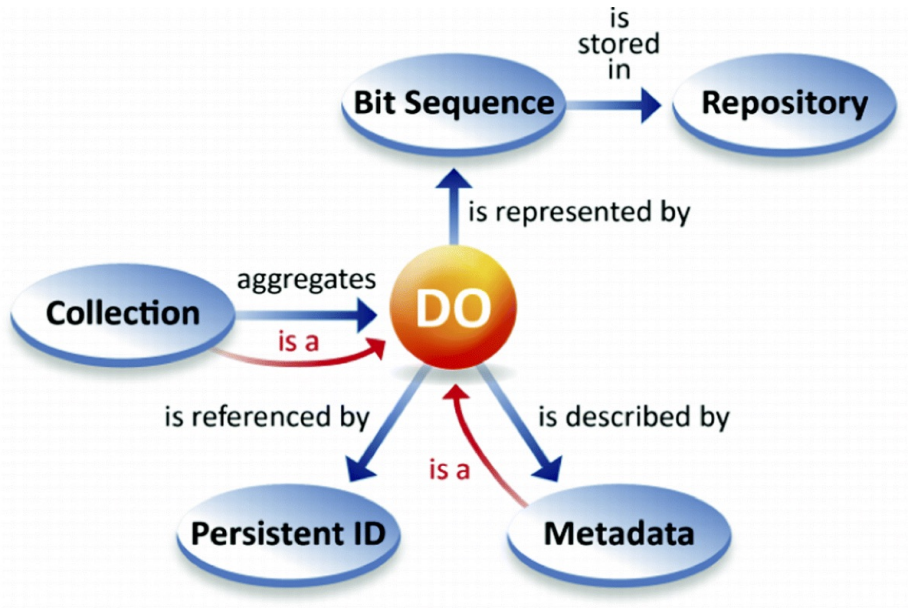
Onafhankelijkheid in het gebruik van standaarden

We zijn van mening dat we niet kunnen standaardiseren naar één standaard. Met standaarden bedoelen we de standaarden die in de technische zorginfrastructuur worden gehanteerd (zie ook het thema open standaarden). We zullen in de tijd gezien altijd meerdere standaarden hebben. Een bronhouder moet daarom aangeven op welke manier data toegankelijk is en welke formaten beschikbaar zijn.

We geven hieronder het voorbeeld van FAIR Digital Object als manier om onafhankelijkheid te verkrijgen.

> **Het voorbeeld van een FAIR Digital Object**
>
> Een digitaal object bestaat uit:
>
> - Data als een verzameling bits.
> - Een unieke vaste identiteit voor het object zodat naar het object kan worden gerefereerd.
> - Formaten waarin de data kan worden weergegeven en de serialisaties waarmee de data kan worden omgezet naar het formaat. Data en representatie staan dus los van elkaar.
> - Metadata waarin onder andere wordt aangegeven wie de bronhouder, wat de gehanteerde ontologie is is en hoe het object toegankelijk is. Onder toegankelijkheid verstaan we ook de verschillende standaarden en protocollen die voor het koppelvlak worden gehanteerd.

> In onderstaand figuur is bovenstaande weergegeven.



Figuur 1: FAIR Digital Object

Bron figuur 1: https://link.springer.com/chapter/10.1007/978-3-030-23584-0_1

FAIR-data

FAIR staat voor vindbaar (Findable), toegankelijk (Accessible), interoperabel (Interoperable), en herbruikbaar (Reusable). Waarom is het belangrijk dat data FAIR is?

Waarom FAIR-data?

Gezondheidsdata moet FAIR zijn stelt de minister. Maar waarom? Een van de doelstellingen voor het informatiestelsel is meervoudig gebruik van data. Herbruikbaarheid van data moet leiden tot lagere kosten en de mogelijkheden openen voor het uitvoeren van onderzoek. We willen daarom dat data vindbaar, toegankelijk en uitwisselbaar is zodat data herbruikbaar is.

De FAIR-dataprincipes zijn internationaal geverifieerde en geaccepteerde principes. Ze dienen als uitgangspunt om data geschikt te maken voor hergebruik.

> **The FAIR Guiding Principles**
>
> To be Findable:
>
> - F1. (meta)data are assigned a globally unique and persistent identifier
> - F2. data are described with rich metadata (defined by R1 below)
> - F3. metadata clearly and explicitly include the identifier of the data it describes
> - F4. (meta)data are registered or indexed in a searchable resource
>
> To be Accessible:
>
> - A1. (meta)data are retrievable by their identifier using a standardized communications protocol
> - A1.1 the protocol is open, free, and universally implementable
> - A1.2 the protocol allows for an authentication and authorization procedure, where necessary
> - A2. metadata are accessible, even when the data are no longer available
>
> To be Interoperable:
>
> - I1. (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.
> - I2. (meta)data use vocabularies that follow FAIR principles
> - I3. (meta)data include qualified references to other (meta)data
>
> To be Reusable:
>
> - R1. meta(data) are richly described with a plurality of accurate and relevant attributes
> - R1.1. (meta)data are released with a clear and accessible data usage license
> - R1.2. (meta)data are associated with detailed provenance
> - R1.3. (meta)data meet domain-relevant community standards
>
> Bron: The FAIR Guiding Principles for scientific data management and stewardship

Open standaarden

In dit hoofdstuk beschrijven we het thema open standaarden. Wat bedoelen we met open standaarden en waarom hebben internationale standaarden voorrang boven nationale standaarden.

Wat zijn open standaarden?

Forum standaardisatie definieert een standaard als een afspraak die is vastgelegd in een specificatiedocument. Om gegevens uit te wisselen moeten ICT-systemen dezelfde standaard hebben geïmplementeerd. Voorwaarde is dan wel dat het specificatiedocument vrij te verkrijgen is.

Forum Standaardisatie hanteert vier kenmerken waaraan een standaard moet voldoen om als 'open standaard' aangemerkt te worden.

- De benodigde documentatie moet laagdrempelig beschikbaar zijn.
- Er mogen geen hindernissen zijn op het terrein van intellectueel eigendomsrecht.
- Er moeten voldoende inspraakmogelijkheden zijn voor stakeholders tijdens de (door)ontwikkeling van de standaard.
- De onafhankelijkheid en duurzaamheid van de standaardisatieorganisatie moeten verzekerd zijn.

Voor de publieke sector hanteert Forum standaardisatie een lijst van open standaarden. We zijn van mening dat voor de gezondheidszorg ook een lijst zou moeten worden onderhouden met de open standaarden die voor de zorg van toepassing zijn.

Waarom internationale standaarden?

Wanneer we als IT-Architecten spreken over open standaarden, dan spreken we over de standaarden die gebruikt worden voor het realiseren van semantische en technische interoperabiliteit. Het gebruik van internationale standaarden is hierbij het uitgangspunt.

- **Internationale standaarden zijn nodig omdat zorg niet gebonden is aan Nederland**. Zeker niet als iemand dicht bij de grens woont. Maar ook toeristen en patiënten met complexe aandoeningen. Zij kunnen in andere landen worden behandeld dan het thuisland. Het uitwisselen van gegevens moet dan ook internationaal worden gedaan. Niet voor niets worden ook in Europees verband standaarden gedefinieerd.
- **Internationale standaarden zijn nodig omdat we gebruik willen maken van de internationale innovatiekracht** op het gebied van informatietechnologie. Het moet voor internationale leveranciers technisch eenvoudig zijn om de Nederlandse markt te betreden.

A1 Netwerkautoriteit

De netwerkautoriteit is verantwoordelijk voor het verkrijgen en behouden van het vertrouwen in het netwerk.

Inleiding

De rol die we beschrijven in dit hoofdstuk is de netwerkautoriteit. De netwerkautoriteit voert de governance over de afspraken. Dat is alles. Ben en Amber zijn met elkaar in gesprek over de rollen en richtlijnen in DIZRA. Ben is programmamanager voor een afsprakenstelsel en Amber is de IT-Architect van het programma. De netwerkautoriteit hoeft niet één organisatie te zijn. We zien juist dat de governance verdeeld is.

De governance kan onderverdeeld worden naar:

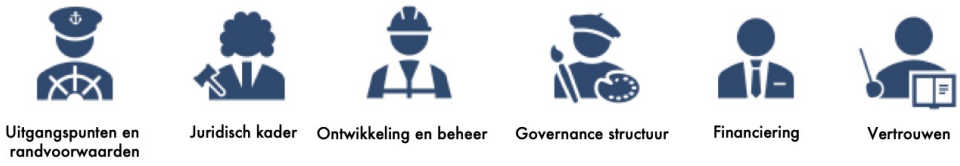
1. Governance op de afspraken voor het registreren van een identiteit;
2. Governance op de afspraken voor de leveranciers van techniek;
3. Governance op de afspraken over interoperabiliteit tussen de netwerkactoren;
4. Governance op de afspraken die het vertrouwen borgen tussen netwerkactoren;
5. Governance op het raamwerk.

De netwerkautoriteit is verantwoordelijk voor het verkrijgen en behouden van het vertrouwen in het netwerk. Zij voert de governance uit op de afspraken en voert regie op de implementatie van de afspraken. Voor het uitvoeren van de vertrouwensdiensten maakt de governance autoriteit gebruik van netwerkbeheerders.

Interoperabiliteit vereist dat er afspraken worden gemaakt op alle lagen van interoperabiliteit. Het is echter mogelijk een scheiding te maken in governance op afspraken over juridische, organisatorische en semantische interoperabiliteit en governance op technische interoperabiliteit. Voor de lagen van interoperabiliteit hanteren we de lagen uit de European Interoperability Reference Architecture (EIRA) en het European Interoperability Framework (EIF). Dat zijn de Europese standaarden voor interoperabiliteit.

Wat voor afspraken moeten we maken?

Welke afspraken moeten gemaakt worden is de vraag van Ben. De afspraken kunnen uiteraard van geval tot geval verschillen vertelt Amber. Er is ook niet één manier die het beste is. We onderkennen zes onderwerpen waarvoor afspraken gemaakt moeten worden.



Figuur 1: Onderwerpen waarvoor afspraken gemaakt moeten worden

De onderwerpen zijn:

- **Uitgangspunten en randvoorwaarden** voor de afspraken;
- **Juridisch kader** van de afspraken;
- Afspraken over de **ontwikkeling en het beheer** van de afspraken;
- De **governance structuur** voor de afspraken met de rollen en verantwoordelijkheden;
- De **financiering** voor de governance, de ontwikkeling en het beheer van de afspraken;
- Afspraken voor het **vertrouwen**. Wie wordt in het netwerk vertrouwd voor het uitgeven van een attest en hoe kan dit geverifieerd worden?

Er zijn inmiddels goede voorbeelden beschikbaar voor deze onderwerpen. MedMij is het meest bekende voorbeeld.

Richtlijnen in de context van de netwerkautoriteit

De onderstaande richtlijnen zijn van toepassing voor de netwerkautoriteit.

A1.1: Het afsprakenstelsel *MOET* voldoen aan de principes.

Het is uitgangspunt dat een afsprakenstelsel de principes hanteert zoals beschreven in het manifest en uitgewerkt in de thema's. Een netwerkautoriteit moet deze principes bewaken en borgen.

A1.2: Het afsprakenstelsel *MOET* voorzien in afspraken over de governance van de afspraken.

We onderkennen twee lagen van afspraken. Afspraken voor de verschillende rollen over vertrouwen, vindbaarheid, toegankelijkheid, interoperabiliteit en herbruikbaarheid. Daarnaast zijn er afspraken over de governance van de afspraken. De netwerkautoriteit moet voorzien in afspraken over governance van de afspraken voor de verschillende rollen in het raamwerk.

A1.3: Het afsprakenstelsel *MOET* voldoen aan de NEN-normen voor medische informatica (NEN-75xx).

De NEN-normen voor medische informatica stellen de functionele en niet-functionele eisen vast voor interoperabiliteit en de ontwikkeling en het beheer van afspraken.

A1.4: Het afsprakenstelsel *MOET* borgen dat een natuurlijk persoon een vrije keuze heeft bij het geven van toestemming.

Een toestemming moet altijd een vrije keuze zijn. Hiervoor zijn afspraken nodig omtrent gedrag en ethiek van deelnemers. Ook zijn afspraken noodzakelijk over een meldpunt en sanctiemaatregelen als afspraken niet worden worden nagekomen.

A1.5: Het afsprakenstelsel *ZOU MOETEN* voorzien in een PDCA-cyclus.

Kwaliteitsbeheersing, kwaliteitsborging, kwaliteitsverbetering zijn voorbeelden van een een continu proces wat vertaald is naar Plan-Do-Check-Act cyclus, oftewel een PDCA-cyclus (kwaliteitscirkel van Deming). Implementatie en beheer zijn onderdeel van deze cirkel.

A2 Auditor

Een auditor is verantwoordelijk voor het uitvoeren van een audit op een rechtspersoon en kan hiervoor een derdenverklaring afgeven of een certificering.

Inleiding

Ben en Amber voeren samen een gesprek over de rollen en richtlijnen. In dit hoofdstuk over de rol van auditor en de afspraken die we voor deze rol moeten maken.

We maken afspraken met elkaar vertelt Amber. We moeten ook verifiëren dat een leverancier of zorginstelling zich houdt aan de afspraken. Inderdaad zegt Ben. Een zorginstelling moet bijvoorbeeld kunnen zien dat een toepassing compliant is aan de afspraken. Een auditor kan die leverancier certificeren zegt Amber. Zo weten we wie wel en wie niet voldoet aan de afspraken.

Wat voor afspraken moeten we maken?

Moeten we afspraken maken met een auditor? Ik denk dat we afspraken moeten maken voor het accrediteren van een auditor zegt Ben. Dat denk ik ook zegt Amber. We zullen dan ook moeten publiceren welke auditors geaccrediteerd zijn.

De auditor voert werkzaamheden uit namens de netwerkautoriteit. Een auditor heeft de volgende verantwoordelijkheden:

- De auditor voert audits uit op de afspraken.
- De auditor controleert dat de netwerkbeheerder, de netwerkactoren, netwerkgids en de techniekleveranciers voldoen aan de afspraken.
- De auditor geeft een derdenverklaring af of certificeert een product.
- De auditor zelf is onderhevig aan accreditatie door de governance autoriteit. De Raad voor Accreditatie zou hier een rol in kunnen spelen. Dit zal moeten worden afgesproken.

Naast de periodieke audit moeten afspraken worden gemaakt over handhaving en toezicht op de uitvoering van de afspraken. Klachten of incidenten moeten bijvoorbeeld kunnen worden geadresseerd aan een toezichthouder / handhaver.

A3 Netwerkactor

Een actor van het ecosysteem is een persoon, apparaat, toepassing, ding dat gebruik maak van het ecosysteem. Zij produceert of consumeert data dan wel stelt services beschikbaar of gebruikt services.

Inleiding

Wat is een netwerkactor? Ben kijkt een beetje vies als hij het woord uitspreekt. Amber moet erom lachen. Netwerkactor is inderdaad een erg abstracte naam. Ben en Amber voeren samen een gesprek over de rollen en richtlijnen. In dit hoofdstuk over de netwerkactor.

Een netwerkactor is iets of iemand. Het zijn alle dingen die een rol spelen in het netwerk en de data die we produceren. Het kunnen rechtspersonen zijn, natuurlijke personen, apparaten, machines en applicaties. Alles wat data produceert of het onderwerp is van data. Maar ook iedereen of alles wat bronhouder is van data of afnemer is van data zegt Amber. Een netwerkactor is niet alleen een organisatie of een mens dus.

> Iedere netwerkactor heeft een eigen identiteit in het netwerk. Als we data produceren willen we weten wie het geproduceerd heeft. Bijvoorbeeld om te weten met welk apparaat een bloeddruk is gemeten. Het apparaat heeft daarom een eigen identiteit nodig zodat we de kennis over het apparaat kunnen beschrijven.

Afspraken maken over rentmeesterschap van data

In navolging van Minister Bruins (Medische Zorg en Sport) zeggen we dat rentmeesterschap op data nodig is. De rol van rentmeester moet daarom worden afgesproken. Om data te laten werken voor gezondheid is vertrouwen nodig.

- Een persoon moet erop kunnen vertrouwen dat er zorgvuldig met zijn/haar data wordt omgegaan
- De zorgverlener moet erop kunnen vertrouwen dat data-analyses valide resultaten opleveren.

Het is de basisgedachte voor het maken van afspraken. Zie het thema data bij de bron.

Afspraken maken over data

DIZRA gaat uit van datagestuurd werken. Dit betekent dat we vanuit de bronhouder data modelleren en beschikbaar stellen. We gaan uit van de beschikbare data bij de bron. Deze data willen we FAIR maken. Vervolgens kunnen we intelligentie op de data toepassen en acties specificeren.

De aanpak komt voort vanuit onze aanname dat we vooraf niet kunnen bedenken wat de vragen zullen zijn. Niet voor niets is het gezegde dat één gek meer kan vragen dat tien wijzen kunnen beantwoorden. Dit is van invloed op de afspraken die we met elkaar maken.

Figuur 1: Datagestuurd werken

Met deze aanpak willen we een aantal doelen bereiken:

- Het beschikbaar stellen van data moet bijdragen aan een versnelling van regie op gegevens. Een bronhouder heeft de data beschikbaar. De data kan via de betrokken persoon of met toestemming van de betrokken persoon worden uitgewisseld.
- Het beschikbaar stellen van data moet bijdragen aan verlaging van de administratieve lasten door eenmalige registratie in de primaire en ondersteunende registraties van een organisatie en meervoudig gebruik van deze gegevens in de administratieve processen, voor het verkrijgen van inzicht en voor het uitvoeren van toezicht (afgeleide stromen: stuur-, beleid-, verantwoording, toezicht- en kwaliteitsinformatie).
- Het beschikbaar stellen van data moet bijdragen aan verlaging van de rapportagelasten door zelfverantwoordelijk rapporteren op basis van de beschikbare data en services. Iedere organisatie kan door de aanpak zelfstandig uitvoering geven aan data-science en data-analyse, waarbij de organisatie zelf verantwoordelijk is voor zowel de vraagstelling als de beantwoording op basis van de voor haar beschikbare gegevens.
- Het beschikbaar stellen van vindbare, toegankelijke, uitwisselbare en herbruikbare data in het netwerk moet leiden tot nieuwe toepassingen die nu veelal nog niet voorzien kunnen worden.

Semantische en technische afspraken maken

We maken afspraken over het beschikbaar stellen van data vertelt Amber. Data FAIR maken noemen we dat. Hiervoor moeten we afspraken maken over de onderstaande onderwerpen.

Figuur 2: Onderwerpen waarvoor afspraken gemaakt moeten worden

De onderwerpen die we onderkennen zijn:

- Afspraken over de indeling van het domein naar **informatiecontexten**. Het domein doet dit al door een verdeling te maken naar onderwerpen zoals: medicatie, verpleging, zwangerschap en geboorte en beelden.
- Afspraken over een **ontologie** (zie ook het thema over een gemeenschappelijke taal). In de ontologie specificeren we de concepten. Op basis van de ontologie kunnen we een attest specificeren.
- Afspraken over de te hanteren **plateaus** voor het vindbaar, toegankelijk en interoperabel maken van data. Een plateau zegt iets over de **volwassenheid** van een organisatie met betrekking tot data. Het plateau is van invloed op de mate van regie op gegevens die de betrokken persoon heeft.
- Afspraken over de **metadata** die beschikbaar worden gesteld en de ontologie van de metadata.
- Afspraken over het beschikbaar stellen van data via een **interface** (zoals HL7 FHIR API), het **dataformaat** en het **transportprotocol**. Dit is afhankelijk van de volwassenheid van een organisatie. Een organisatie kan door een interface data toegankelijk maken. Een hoger niveau van regie op gegevens wordt door een organisatie gerealiseerd als zij een interface biedt voor het uitgeven en ontvangen van attesten.
- Afspraken maken over het beschikbaar stellen van **services** op data, bijvoorbeeld om via querytalen of via algoritmes data beschikbaar te stellen. Dit is afhankelijk van de volwassenheid van een organisatie. Als een organisatie data via een ontologie beschikbaar kan stellen, dan kunnen ze deze toegankelijk maken via een querytaal. Het beschikbaar stellen van een algoritme op de data is weer een stap verder.
- Afspraken maken over het proces en de ontwikkeling van **geautoriseerde uitwisselingen** van data.

> **Wat is een ontologie?**
>
> Je gebruikt woorden die ik niet ken klaagt Ben. Wat is bijvoorbeeld een ontologie? Vroeger maakten we gewoon een datamodel. Bedoel je dat? Het lijkt er inderdaad op zegt Amber. Een ontologie is een conceptueel model. Er worden concepten beschreven en de betekenis van die concepten. Uiteraard gebruiken we woorden om het concept te omschrijven. Met een ontologie zorgen we ervoor dat machines onze logica gaan begrijpen. Kun je een voorbeeld noemen vraagt Ben. Ik vind het nogal vaag wat je vertelt.

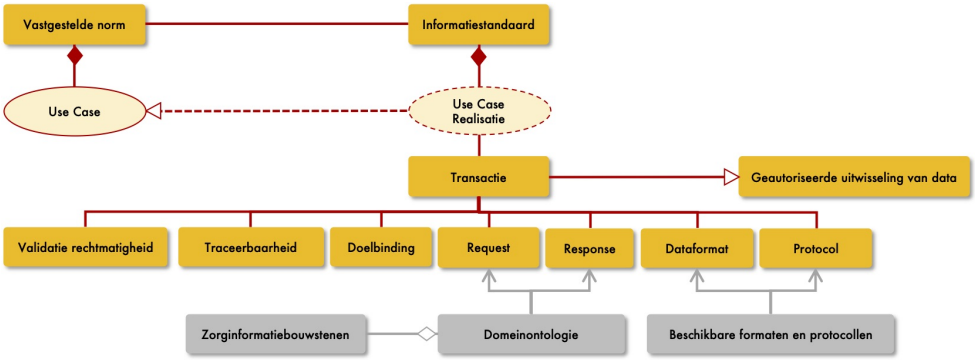
> Als mens weten we wat een patiënt is zegt Amber. Maar een machine weet dat niet. We moeten een machine kunnen uitleggen wat een patiënt is. We moeten de machine uitleggen dat een patiënt een mens is. Maar wat maakt een mens tot een patiënt. Wanneer is een mens een patiënt? We moeten dat specificeren. Dat betekent dat we eerst moeten afspreken wat een concept betekent. De definitie van het concept patiënt moeten we specificeren op een manier die voor mensen en machines te begrijpen is. Dat is een ontologie.

Voordat we verder gaan wil ik eerst nog even iets weten zegt Ben. Je hebt het nu over het beschikbaar stellen van data. Maar het gaat toch over interoperabiliteit? We moeten dus afspraken maken tussen organisaties op alle lagen van interoperabiliteit. Uiteindelijk moeten we berichten specificeren op basis van de data die een zorgprofessional nodig heeft.

We moeten inderdaad OOK afspraken maken over interoperabiliteit zegt Amber. Maar ook over vindbaarheid, toegankelijkheid en herbruikbaarheid. We willen data FAIR beschikbaar stellen per informatiecontext. Daarmee willen we niet alleen de informatiebehoefte van een zorgprofessional invullen, maar ook andere vragen kunnen beantwoorden. Meervoudig gebruik van data noemen we dat.

Geautoriseerde uitwisselingen

Semantische interoperabiliteit bereiken we door het afspreken van een ontologie zegt Amber. Vervolgens kunnen we vragen en antwoorden formuleren op basis van de specificaties in de ontologie. We matchen vraag en aanbod. Voor de verwerking van persoonsgegevens moeten we van een netwerkactor weten waar zij van is en wat zij wel en niet mag. Iedere uitwisseling van persoonlijke data moet verantwoord kunnen worden en moet daarom een geautoriseerde uitwisseling zijn.



Figuur 3: Afspreken geautoriseerde uitwisseling van data

In bovenstaand figuur zijn de onderwerpen opgenomen voor een geautoriseerde uitwisseling. Het ontwikkelen van normen en informatiestandaarden is doelgericht. Voor een use case worden afspraken gemaakt voor juridische en organisatorische interoperabiliteit. De processtappen van een use case beschrijft de uitwisseling van persoonsgegevens. Iedere uitwisseling noemen we een transactie. Een transactie wordt geïnitieerd vanuit een actor. De actor moet een grondslag en een doel hebben voor de verwerking van de persoonsgegevens. Iedere transactie moet verantwoord kunnen worden.

Voor iedere transactie worden minimaal de volgende afspraken gemaakt:

- Afspraken over de **validatie van rechtmatigheid**. Een bronhouder van data moet valideren dat data rechtmatig op basis van de juiste autorisaties bij de juiste persoon komen. Er zijn afspraken nodig om deze validatie gemeenschappelijk te doen voor alle bronhouders.
- Afspraken over **traceerbaarheid** van de transactie naar de natuurlijke persoon die de verwerking initieerde. De traceerbaarheid moet gerealiseerd worden in de log van de transactie. Het is een afspraak die bij voorkeur gemeenschappelijk wordt gemaakt voor alle transacties.
- Afspraken over het **doel** of doelbinding. Het doel is de verantwoording waarom de transactie is uitgevoerd. Het doel moet herleid kunnen worden naar een grondslag, naar de activiteiten van de verwerker en de natuurlijke persoon die de verwerking initieerde. Iedere transactie moet geregistreerd worden in een log.
- Afspraken over het **request en de response** van de transactie. Gezamenlijk met de dataformaten en het protocol vormt dit de interface. Het request en de response moeten worden samengesteld op

basis van de concepten die in de ontologie zijn vastgelegd.
- Afspraken over de **dataformaten** die ondersteund worden, zoals JSON of XML.
- Afspraken over de **protocollen** die ondersteund worden, zoals het HTML-protocol.

De normen en informatiestandaarden kunnen paralel worden ontwikkeld aan de ontwikkeling van de ontologie en het beschikbaar stellen van data. DIZRA hanteert als uitgangspunt dat een techniekleverancier de techniek levert voor technische afspraken.

Afspraken maken over digitale inclusie

Een afsprakenstelsel moet afspraken maken over digitale inclusie. Bijvoorbeeld door aan te sluiten bij het programma digitale inclusie van de overheid. Zie https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/toegankelijkheid/digitale-inclusie/

Richtlijnen in de context van de netwerkactor

De onderstaande richtlijnen zijn van toepassing voor de netwerkactor.

A3.1: Het afsprakenstelsel *MOET* voorzien in afspraken voor een bronhouder over vindbaarheid, toegankelijkheid en interoperabiliteit van data en services.

Een bronhouder moet vindbaar, toegankelijk en interoperabel zijn. Het zijn afspraken over onder andere het realiseren van een ontologie, het beschikbaar stellen van data en metadata en de afspraken over protocollen en dataformaten voor toegang.

A3.2: Het afsprakenstelsel *MOET* voorzien in afspraken over de ontwikkeling en toepassing van geautoriseerde uitwisselingen.

Voor een afsprakenstelsel moeten afspraken worden gemaakt welke rollen worden onderkend voor bronhouders en gegevensafnemers, waar iemand van is, wat die mag en wat die moet doen. Voor ieder van de rollen moet afgesproken worden wat de minimale dataset is die mag worden uitgewisseld.

A3.3: Het afsprakenstelsel *MOET* voldoen aan de NEN-normen voor medische informatica (NEN-75xx).

De NEN-normen voor medische informatica stellen de functionele en niet-functionele eisen vast voor interoperabiliteit tussen netwerkactoren.

A3.4: Het afsprakenstelsel *MOET* afspraken maken over digitale inclusie.

Met de digitalisering willen we niemand uitsluiten. Voor meer informatie over digitale inclusie, zie het thema regie op gezondheidsdata.

A3.5: Het afsprakenstelsel *MOET* voorzien in afspraken over de inrichting van rentmeesterschap van data bij een bronhouder.

In navolging van Minister Bruins (Medische Zorg en Sport) zeggen we in DIZRA dat we rentmeesterschap op data nodig hebben. Om data te laten werken voor gezondheid is vertrouwen nodig. De patiënt moet erop kunnen vertrouwen dat er zorgvuldig met zijn/haar data wordt omgegaan en de zorgverlener moet erop kunnen vertrouwen dat data-analyses valide resultaten opleveren. Zie ook het thema data bij de bron.

A4 Techniekleverancier

Een leverancier van techniek is een actor die onderdelen levert voor het realiseren van technische interoperabiliteit met een netwerk en tussen personen of dingen.

Inleiding

We hebben heel veel leveranciers die iets met techniek doen vertelt Amber. Ben en Amber voeren samen een gesprek over de rollen en richtlijnen. In dit hoofdstuk over de techniekleverancier. Kijk maar hoeveel apparaten en applicaties er zijn in de gezondheidszorg. Maar ook hoeveel diensten voor informatietechnologie er zijn. En al deze dingen en diensten worden geleverd door leveranciers. We noemen ze techniekleveranciers.

Moeten we met al deze leveranciers van techniek afspraken maken en ze gaan certificeren vraagt Ben. Dat is een gigantische klus en ik ben niet overtuigd dat het nodig is. Dat weten we niet zegt Amber. We weten alleen dat we betrouwbare data nodig hebben uit betrouwbare en vertrouwde techniek.

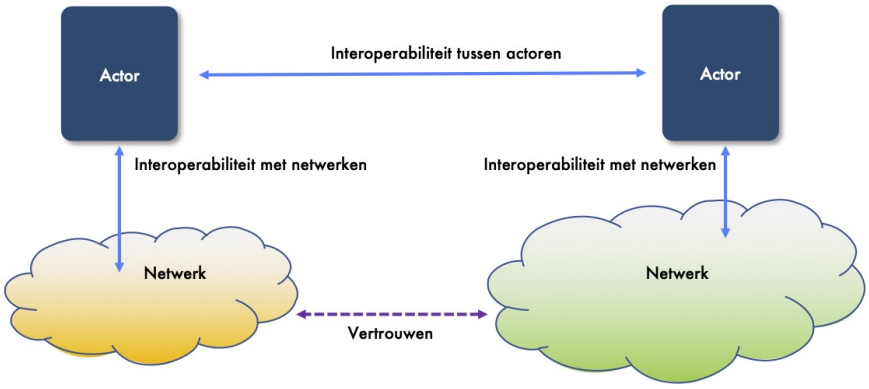
Betrouwbare data begint bij de bron. Afspraken gaan daarom niet alleen om extramurale communicatie van data vervolgt Amber. We moeten ook kijken naar intramurale communicatie van data. Ben kijkt een beetje beteuterd. Het zal een continue ontdekkingstocht zijn om te leren welke data we nodig hebben verzucht hij. Dat klopt zegt Amber. We moeten leren welke data we kunnen en willen hergebruiken, wat relevant is en welke afspraken nodig zijn.

Een techniekleverancier en de dienstverlener zorgaanbieder

Nog een vraag zegt Ben. Is een dienstverlener zorgaanbieder hetzelfde als een techniekleverancier? Bedoel je daar hetzelfde mee? Nee zegt Amber. Een dienstverlener zorgaanbieder is een rol in het afsprakenstelsel MedMij. Het is een leverancier van techniek die de technologie en diensten levert om een persoonlijke gezondheidsomgeving aan te sluiten op de systemen van een zorgaanbieder. Het is een specialisatie binnen de verzameling techniekleveranciers.

Wat voor afspraken moeten we maken?

Een rechtspersoon, natuurlijk persoon, apparaat of ding maakt gebruik van software en hardware om elektronisch verbinding te maken met andere personen, apparaten of dingen. Maar ook om verbinding te maken met de services van een netwerkbeheerder. Leveranciers van techniek leveren de software en de hardware die dit mogelijk maakt. Iedere rechtspersoon en/of natuurlijk persoon kiest haar eigen leveranciers in een gelijk speelveld.



Figuur 1: Technische interoperabiliteit tussen personen en netwerk

Wat betekent dit?

> Bob is apotheker. Hij wisselt met verschillende zorgverleners (voorschrijvers) gegevens uit om geneesmiddelen te verstrekken. Maar ook met patiënten. Om met iedereen elektronisch te kunnen communiceren heeft Bob software aangeschaft.
>
> Bob heeft voor zijn patiënten een apparaat op de balie staan waarmee berichten kunnen worden uitgewisseld met de telefoon van de patiënt. Via het apparaat kunnen ook berichten naar de telefoon worden verzonden.
>
> Bob heeft verschillende toepassingen aangeschaft van verschillende soft- en hardwareleveranciers. Dit zijn allemaal leveranciers van techniek. Zijn apotheek heeft zelf geen IT-afdeling, maar maakt gebruik van een dienstverlenende organisatie voor informatietechnologie. Deze organisatie implementeert de toepassingen in zijn apotheek en is daarmee ook een leverancier van techniek.

We moeten met leveranciers afspraken maken om compliant te zijn aan de afspraken voor semantische en technische interoperabiliteit. Met een derdenverklaring van een auditor kan de software en hardware van de leverancier gecertificeerd worden voor gebruik.

Richtlijnen in de context van de techniekleverancier

De onderstaande richtlijnen zijn van toepassing voor de techniekleverancier.

A4.1: Het afsprakenstelsel *MOET* voorzien in afspraken dat producten van techniekleveranciers personen in staat stellen regie te nemen op gegevens.

De producten van een techniekleverancier moeten personen in staat stellen regie te nemen op zijn of haar gegevens. Het product moet daarom functionele ondersteuning geven aan het uitgeven, het houden dan wel het verifiëren van een attest. Voor het verifiëren van een attest moet het product interoperabel zijn met de diensten van een netwerkbeheerder.

A4.2: Het afsprakenstelsel *MOET* voorzien in afspraken dat producten van techniekleveranciers gegevenselementen kunnen interpreteren overeenkomstig de ontologie van het domein.

Voor eenheid van taal en interpretatie hanteren bronhouders een gemeenschappelijke ontologie (zie het thema gemeenschappelijke taal). Een ontologie wordt afgesproken binnen een informatiecontext in een domein. De data is uitwisselbaar en machineleesbaar doordat de data gepubliceerd is in de ontologie. Een product van een techniekleverancier moet haar gegevenselementen kunnen interpreteren overeenkomstig de ontologie.

A4.3: Het afsprakenstelsel *MOET* voorzien in afspraken dat producten van techniekleveranciers data kunnen extraheren en laden overeenkomstig de ontologie van het domein.

DIZRA gaat uit van FAIR-data waarbij data hergebruikt kan worden. Eenmalige registratie, meervoudig gebruik is het doel. Hiervoor is het noodzakelijk dat producten open zijn voor het extraheren en laden van data. Zodat we de data kunnen hergebruiken.

A4.4: Het afsprakenstelsel *MOET* voorzien in afspraken dat producten van techniekleveranciers voldoen aan de toegankelijkheidsstandaard EN 301 549 (waaronder de WCAG webrichtlijnen) indien gebruik wordt gemaakt van een eindgebruikersinterface op een mobiel apparaat of webinterface.

In het tijdelijk besluit digitale toegankelijkheid overheid is EN 301 549 aangewezen als verplicht toe te passen standaard voor organisaties met een wettelijke taak. Voor de toepassingen in de zorg stelt DIZRA

het als richtlijn vast. Regie op gegevens kan namelijk pas bestaan als we bruikbare toepassingen hebben om regie mee te voeren.

A4.5: Het afsprakenstelsel *MOET* voorzien in afspraken dat producten van techniekleveranciers voldoen aan de NEN-normen voor medische informatica (NEN-75xx).

De NEN-normen voor medische informatica stellen de functionele en niet-functionele eisen vast voor interoperabiliteit tussen netwerkactoren. Een techniekleverancier moet de eisen ten aanzien van technische interoperabiliteit invullen.

A4.6: Het afsprakenstelsel *MOET* voorzien in afspraken dat producten van techniekleveranciers open internationale standaarden hanteren voor interoperabiliteit.

We hanteren standaarden voor interoperabiliteit, geen producten. Een product van een techniekleverancier kan niet de standaard zijn volgens de principes van DIZRA. Daarom moeten de producten open internationale standaarden hanteren voor het publiceren, toegankelijk maken en uitwisselen van data. Voor meer informatie, zie het thema open standaarden.

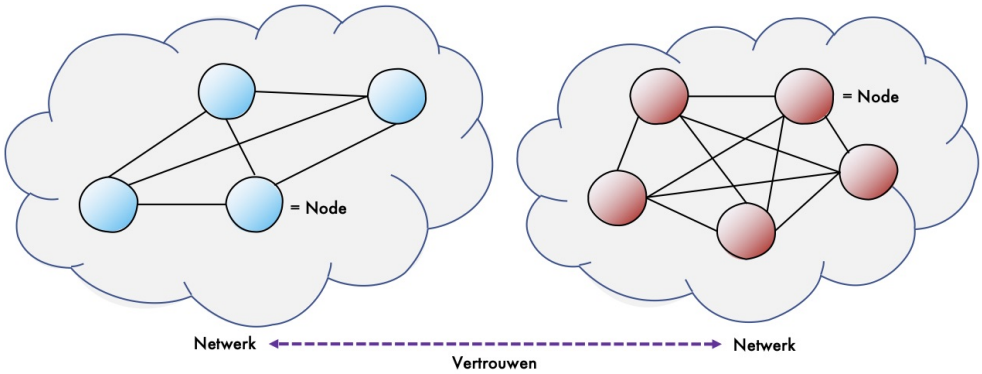
A5 Netwerkbeheerder

Een netwerkbeheerder is een actor die alleen of samen met andere netwerkbeheerders een netwerk implementeert en operationeel houdt. Zij levert de dienste voor het realiseren van een vertrouwd netwerk.

Inleiding

Verantwoord beheer en gebruik van data begint met vertrouwen. Vertrouwen in de actoren die gebruik willen maken van data. Daarom is een vertrouwd netwerk van actoren nodig. Een netwerk bestaat uit een of meerdere nodes (knooppunten) waarop vertrouwensdiensten worden aangeboden. Het zijn vertrouwensdiensten met betrekking tot de identiteit van een actor en de attesten die worden uitgegeven als verklaring over een actor. Een attest is een elektronisch bewijs, een (officiële) verklaring die een bewering versterkt, ondersteunt, wettigt. Een attest kan gebruikt worden voor de authenticatie van een persoon.

De netwerkbeheerder voert de processen uit en hanteert voorwaarden voor deelname aan het netwerk. Iedere node wordt uitgevoerd door een netwerkbeheerder. Een aanname is dat er meerdere netwerken zullen zijn. Dat er ook meerdere netwerkbeheerders kunnen zijn in een netwerk. Uitgangspunt is dat actoren zich kunnen aanmelden bij het netwerk en de netwerkbeheerder van hun keuze. We denken bijvoorbeeld aan een netwerk voor gemeenten, aan een netwerk voor dingen, aan regionale netwerken en aan netwerken voor natuurlijke personen. Een netwerk kan met of zonder winstoogmerk zijn opgezet.



Figuur 1: Een actor moet een auteur vertrouwen en daarmee het netwerk van de auteur

Om een attest te vertrouwen moet een actor de uitgever vertrouwen. Ieder netwerk maakt afspraken over de uitgevers die zij vertrouwt. Andere netwerken kunnen deze afspraken overnemen.

Vertrouwen en regie op gegevens

Een netwerkbeheerder levert vertrouwensdiensten. Het is een vertrouwensdienst waarmee de identiteit van een netwerkactor wordt geregistreerd. Maar alleen voor actoren waarvan de identiteit herleid moeten kunnen worden. Publieke actoren noemen we deze, in tegenstelling tot private actoren. Een actor is bijvoorbeeld publiek omdat de herkomst van data geverifieerd moet kunnen worden. Authenticatie dus zegt Ben. Het is inderdaad een vorm van authenticatie zegt Amber.

Met de dienst voor elektronische ondertekening kunnen we bijvoorbeeld regie op gegevens realiseren. Het maakt het mogelijk dat je als persoon een bewering doet (ik ben 18, ik heb mijn rijbewijs, ik heb een zorgindicatie) en een bevoegde instantie deze bewering attesteert door de bewering elektronisch te ondertekenen. De bewering is verifieerbaar geworden omdat de bevoegde instantie een geregistreerde netwerkactor is.

Richtlijnen in de context van de netwerkbeheerder

Een netwerkbeheerder levert diensten aan personen. Dit zijn zowel rechtspersonen als natuurlijke personen. De netwerkbeheerder stemt haar diensten af op haar klanten en de vraag van haar klanten.

A5.1: Het afsprakenstelsel *MOET* afspraken bevatten voor een dienst voor het registreren van een identiteit.

Een persoon moet in het netwerk een identiteit kunnen verkrijgen. Met persoon bedoelen we zowel rechtspersonen als natuurlijke personen. De persoon is met die identiteit bekend in het netwerk. De identiteit wordt onder andere gebruikt voor het uitgeven van een attest. Een persoon wordt alleen geregistreerd als iemand of iets de betrouwbaarheid van de identiteit van de persoon moet kunnen verifiëren. Hiermee ontstaat een netwerk van vertrouwde deelnemers.

Het verkrijgen van een identiteit in het netwerk kan aan voorwaarden gebonden zijn. Een netwerk kan bijvoorbeeld besloten zijn voor een specifieke groep uitgevers of kan eisen stellen aan de technische infrastructuur van een uitgever.

> **Centrale, federatieve en decentrale identiteiten**
>
> Identiteit en toegangsbeheer kan op verschillende manieren worden ingevuld. We zien centrale, federatieve en decentrale oplossingen.
>
> Centrale en federatieve oplossingen gaan uit van een identificatiemiddel als product. Het product moet door iedereen gebruikt gaan worden. Een persoon heeft daardoor een veelheid aan producten waarmee zij zich kan identificeren. We zien producten zoals DigiD, eHerkenning en iDin. Daarnaast gebruiken mensen ook de producten van Google en Facebook om zich te identificeren.
>
> We denken dat het stapelen van producten niet houdbaar is en niet duurzaam. We zijn van mening dat er vanuit een actor gedacht moet worden, iemand of iets met een identiteit. Een actor moet soeverein zijn in het maken van haar eigen identiteit.
>
> **Identificatie en authenticatie**
>
> We specificeren identificatie en authenticatie omdat het vaak tot verwarring leidt. Met een identiteit doelen we op een betekenisloos nummer in combinatie met een cryptografische sleutel. Met de sleutel kan de herkomst van data bewezen worden. Authenticatie is in dit geval de verificatie dat iemand of iets de controle heeft over de sleutel.
>
> Naast de identiteit zijn er de gegevenselementen. Bijvoorbeeld een klantnummer. Met authenticatie bedoelen we meestal dat we willen bewijzen dat iemand de controle heeft over het klantnummer en deze mag gebruiken. Het is een verificatie van een bewering. Daarom is authenticatie veelal gelijk aan het verifiëren van een attest.

A5.2: Het afsprakenstelsel *MOET* een open internationale standaard hanteren als methode voor de registratie van een identiteit.

DIZRA hanteert als uitgangspunt dat er meerdere netwerken naast elkaar bestaan. Iedere uitgever moet echter herkenbaar zijn als een uitgever die erkend is en vertrouwd is in een netwerk. De methode van registratie moet borgen dat het netwerk van de uitgever bekend is. Een Uniform Resource Name (URN) is bijvoorbeeld de meest gehanteerde methode om het netwerk te herkennen.

A5.3: Het afsprakenstelsel *MOET* een authenticatiemiddel afspreken met een hoog identiteitsbetrouwbaarheidsniveau.

Met de identiteit verkrijgt de rechtspersoon een middel waarmee zij kan bewijzen eigenaar te zijn van de identiteit. De rechtspersoon moet kunnen aantonen dat zij de controle heeft over de identiteit. De identiteit en het middel moeten op een hoog identiteitsbetrouwbaarheidsniveau kunnen worden toegepast.

Voor het vaststellen van het identiteitsbetrouwbaarheidsniveau hanteren we de regels uit verordening (EU) 910/2014 van het Europees Parlement en de Raad van 23 juli 2014.

A5.4: Het afsprakenstelsel *MOET* een middel afspreken voor het plaatsten van gekwalificeerde elektronische handtekeningen.

Door de elektronische handtekening kan een uitgever van een attest data elektronisch ondertekenen en daarmee de herkomst van de data vastleggen. Een verificateur kan op basis van de elektronische handtekening de herkomst vaststellen.

Een gekwalificeerde elektronische handtekening is een elektronische handtekening die voldoet aan de eisen van Verordening (EU) nr. 910/2014 (eIDAS Verordening). Kwalificatie van het middel is optioneel en alleen van toepassing als de herkomst van data onweerlegbaar moet worden bewezen.

A5.5: Het afsprakenstelsel *MOET* een dienst afspreken voor het intrekken en het verifiëren van de geldigheid van een attest.

Met de verificatie moet een verificateur van een attest kunnen verifiëren dat data afkomstig is van een vertrouwde uitgever. Een netwerkbeheerder moet daarom registreren welke uitgever vertrouwd wordt voor het uitgeven van welke attesten. De verificateur van het attest moet eveneens kunnen verifiëren dat het attest geldig is, en niet is ingetrokken.

A6 Netwerkgids

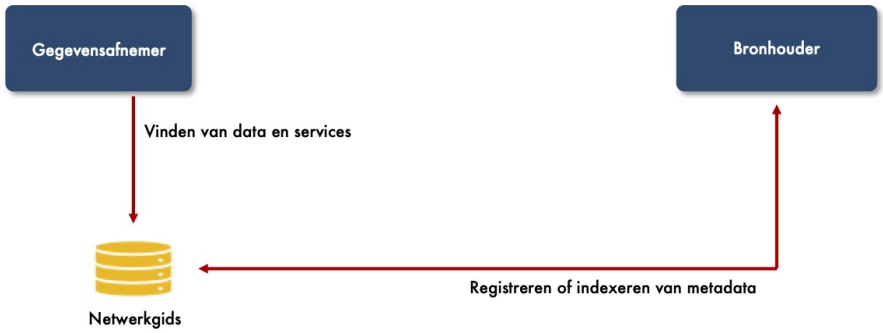
De netwerkgids zorgt ervoor dat data en services in het netwerk.gevonden kunnen worden.

Inleiding

Een aantal netwerkactoren moet ook vindbaar zijn vertelt Amber. Wat bedoel je daarmee vraagt Ben. Ben en Amber voeren samen een gesprek over de rollen en richtlijnen. In dit hoofdstuk over de netwerkgids. Als ik bijvoorbeeld met mijn huisarts gegevens wil uitwisselen, dan moet ik het elektronische adres hebben zegt Amber. De eenvoudige manier is om naar de website van de huisarts te gaan en met mijn mobiel een QR-code te scannen. Maar je kunt je voorstellen dat dat voor zorgprofessionals in een ziekenhuis niet echt werkt. Zij kunnen niet iedere keer naar een website gaan om een huisarts op te zoeken. De netwerkgids zorgt ervoor dat elektronische adressen doorzoekbaar zijn op basis van verschillende zoekcriteria.

Wat voor afspraken moeten we maken?

Binnen het netwerk moeten data en services gevonden kunnen worden. Het is één van de principes van FAIR-data. De netwerkgids is de rol binnen het netwerk die de services biedt voor het vinden. In onderstaande figuur zijn de services weergegeven.



Figuur 1: Services van de netwerkgids

Richtlijnen in de context van de netwerkgids

De onderstaande richtlijnen zijn van toepassing voor de netwerkgids.

A6.1: Het afsprakenstelsel *MOET* een dienst afspreken voor het vinden van data en services.

De netwerkgids biedt een service aan voor het zoeken van een technisch adres. Het zoeken en vinden van de data en services wordt uitgevoerd op basis van de metadata die beschikbaar is gesteld. Een voorbeeld van een technisch adres is een Uniform Resource Locator (URL). Het is het adres waarop data dan wel een service toegankelijk is.

De principes van FAIR-data laten een keuze tussen registratie en indexatie van metadata. De metadata is de brondata voor het zoeken en vinden van data en services. De metadata wordt geregistreerd of geïndexeerd in doorzoekbare bron.